N° d'ordre 127 Année 2015

جامعة عبد المالك السعدي
Université Abdelmalek Essaadi

UNIVERSITE ABDELMALEK ESSAADI
FACULTE DES SCIENCES et TECHNIQUES
TANGER

Centre d'Etudes Doctorales : « Sciences et Techniques de l'Ingénieur »
Formation Doctorale : « Sciences et Techniques de l'Ingénieur »

THESE DE DOCTORAT

Présentée

Pour l'obtention du

DOCTORAT EN SCIENCES ET TECHNIQUES DE L'INGENIEUR

Par :
RGHIOUI Anass

Discipline : Informatique et Télécommunication

Spécialité : Réseaux, Informatique et Télécommunication

Titre de la Thèse :

Contribution aux réseaux 6LoWPAN : Sécurisation des applications de l'e-santé dans le contexte de l'Internet des Objets

Soutenue le 15/09/2015 devant le Jury

Président :
Pr. ADDOU Mohamed (Doyen de la Faculté des Sciences et Techniques - Tanger)
Rapporteurs :
Pr. AKNIN Nora (Faculté des Sciences - Tétouan)
Pr. FENNAN Abdelhadi (Faculté des Sciences et Techniques - Tanger)
Pr. SAYOUTI Adil (École Royale Navale - Casablanca)
Examinateur :
Pr. ELOUAI Fatiha (Faculté des Sciences et Techniques - Tanger)
Directeur de thèse :
Pr. BOUHORMA Mohammed (Faculté des Sciences et Techniques - Tanger)

Structure de recherche accréditée d'accueil :
UAE/L08FST : Laboratoire d'Informatique, Systèmes et Télécommunication
de la Faculté des Sciences et Techniques de Tanger

Contribution to 6LoWPAN networks: Securing the Internet of e-healthcare Things

A DISSERTATION PRESENTED

BY

ANASS RGHIOUI

TO

THE COMPUTER SCIENCE DEPARTMENT

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

PHILOSOPHIÆ DOCTOR

IN THE SUBJECT OF

COMPUTER SCIENCE, NETWORKS & TELECOMMUNICATIONS

ABDELMALEK ESSAADI UNIVERSITY

FACULTY OF SCIENCE AND TECHNOLOGY, TANGIER

2015

Laboratoire d'Informatique, Systèmes et Télécommunication
Faculté des Sciences et Techniques de tanger
Université Abdelmalek Essaadi, Maroc

Le candidat a bénéficié d'une ***bourse d'excellence*** *octroyée par le Centre National pour la Recherche Scientifique et Technique et ce dans le cadre du programme des bourses de recherche initié par le Ministère de l'Education Nationale, de l'Enseignement Supérieur, de la Formation des Cadres et de la Recherche Scientifique.*

Laboratory of Informatics, Systems and Telecommunications
Faculty of Science and Technology of Tangier
Abdelmalek Essaadi University, Morocco

The candidate benefited from the "Bourse d'excellence" scholarship awarded by the National Center for Scientific and Technical Research "CNRST" and the program of research grants initiated by the Minister of Higher Education, Executive Training and Scientifc Research "ENSSUP".

To my parents,
my brother & my sisters,
my wife
& my children

Thesis advisor: Mohammed BOUHORMA Anass RGHIOUI

Contribution to 6LoWPAN networks: Securing the Internet of e-healthcare Things

Abstract

The development of the Internet of Things and its application in the field of healthcare will greatly serve the process of diagnosis and facilitate the monitoring of patients with small IP-based wireless sensors placed on the patient's body. The set of physiological parameters such as blood pressure, heart rate and rhythm, etc., can be monitored remotely and continuously. This application must absolutely maintains the confidentiality of medical information relating to patients, only caregivers should be allowed to access this information. Security must be ensured throughout all the care process.

With 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) technology, the concept of the Internet of Things has been a reality; each object may have an IPv6 address, which will allow him to connect to the world of the Internet. Nevertheless, in the field of research, the main goal of researchers in the design of a new technology is to provide an efficient and economical system, that security dimension is generally neglected, which opens the door to different threats due to the vulnerability of the system.

Objects in the world of the Internet of Things are heterogeneous; they vary according to their roles, their material resources and their operation. They are spread everywhere, and information provided by the Internet between two distinct objects is insecure, vulnerable to eavesdropping or to external attacks. This enforces

to improve the security system in order to preserve the integrity and protect the confidentiality of data exchanged by the establishment of an end-to-end security system.

The 6LoWPAN combines between two different networks: the IEEE 802.15.4 and the IPv6. For its security, we need a solution that addresses both internal communications and those across the Internet. Existing solutions address the security of a communication type separately from the other, where we must implement several solutions to secure a single network, which is not practical for networks with limited resources.

In this thesis, we offer a security solution for 6LoWPAN networks, based on the use of a remote server to manage cryptography keys and authentication. The solution aims to ensure internal communications and end-to-end communications. Our simulations and performance analysis shows that our solution provides security and is effective in computing, communication and storage. However, cryptography protects the network only from outside attackers so that a compromise node can launch attacks from the inside and will not be detected because it is considered a legitimate node, mainly for 6LoWPAN devices that are deployed in an insecure environment. To remedy this problem, an intrusion detection system (IDS) should be used as a second line of defense and a wall against internal threats. We give a preliminary study on the IDS approaches proposed for the resource-constrained networks, to choose the most appropriate system to use for 6LoWPAN networks. In addition, we propose an IDS system well suited for 6LoWPAN networks.

The main goal of our contribution is to secure the e-healthcare applications in the world of the Internet of Things, by protecting data confidentiality and ensuring system availability while minimizing energy consumption.

Contribution aux réseaux 6LoWPAN: Sécurisation des applications de l'e-santé dans le contexte de l'Internet des Objets

Résumé

Le développement de l'Internet des Objets et son application dans le domaine de la santé va grandement servir au processus du diagnostic et facilitera le suivi des patients à l'aide de petits capteurs sans fil basés sur IP placés sur le corps du patient. L'ensemble des paramètres physiologiques tels la pression artérielle, le rythme et la fréquence cardiaque, etc., peuvent être surveillés à distance et en continu.

Cette application doit absolument respecter la confidentialité des informations médicales liées aux patients, aux soignants et seules les intervenants aux soins sont autorisées d'accéder à cette base d'informations. La sécurité doit être assurée tout au long de la démarche des soins. Grâce à 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks), le concept de l'Internet des Objets a pu voir le jour, chaque objet aura une adresse IPv6, ce qui lui permettra d'intégrer le monde de l'Internet. Cette offre permet aux objets de recueillir et de surveiller les données à distance. Pourtant, dans le domaine de la recherche, le principal objectif des chercheurs lors de la conception d'une nouvelle technologie est d'offrir un système efficace et économique, ce qui fait que la dimension sécurité est généralement négligée, ce qui ouvre la porte aux menaces de sécurité devant la vulnérabilité du système.

Les objets dans le monde de l'Internet des Objets sont hétérogènes, ils varient

en fonction de leurs rôles, leurs ressources matérielles et de leur fonctionnement. Ils sont répandues partout et l'information communiquées par Internet entre deux objets distincts n'est pas sécurisé voir vulnérable à une écoute sans autorisation ou à une attaque externe. Ceci impose d'améliorer la sécurité dans ce système afin de préserver l'intégrité et de protéger la confidentialité des données échangées par la mise en place d'un système de sécurité de bout-en-bout.

Le 6LoWPAN combine entre deux réseaux différents : LoWPAN et IPv6, pour sa sécurité, nous avons besoin d'une solution qui traite à la fois les communications internes et ceux à travers l'Internet. Les solutions existantes traitent la sécurité d'un type de communication séparément des autres, où nous devons mettre en œuvre plusieurs solutions pour sécuriser un réseau unique, ce qui n'est pas pratique pour les réseaux avec contraintes de ressources.

Nous proposons une solution adaptée aux réseaux 6LoWPAN, basé sur l'utilisation d'un serveur distant pour gérer les clés de sécurité et l'authentification des nœuds. La solution vise à garantir les communications internes et les communications de bout-en-bout. Nos simulations et analyse de la performance montre que notre solution assure la sécurité, et elle est efficace en énergie. Cependant, la cryptographie protège le réseau uniquement des attaquants externes alors qu'un nœud compromis peut lancer des attaques de l'intérieur et ne sera pas détecté car il est considéré comme un nœud légitime, surtout les dispositifs 6LoWPAN qui sont déployés dans un environnement hostile. Afin de remédier à ce problème, un système de détection d'intrusion (IDS) doit être utilisé comme une deuxième ligne de défense et un mur contre les menaces internes. Nous donnons une

étude préliminaire sur les systèmes IDS qui sont proposées pour les réseaux de ressources limitées afin de choisir le système le plus adéquat pour l'utiliser pour les réseaux 6LoWPAN. En outre, nous proposons un système IDS bien adapté pour les réseaux 6LoWPAN.

L'objectif principal de notre contribution est de sécuriser les applications d'e-santé dans le monde de l'Internet des Objets, en protégeant la confidentialité des données et d'assurer la disponibilité du système, tout en minimisant la consommation d'énergie.

Contents

Listing of figures

Acknowledgments

Thank priority Allah, the Almighty, for giving me the courage, strength and the will to complete this work.

I express my thanks to my supervisor Professor BOUHORMA Mohammed for his support, his kindness and generosity during all these years.

My thanks to Mr. ADDOU Mohamed, president of the jury and Dean of the Faculty of Science and Technology of Tangier.

Mr. SAYOUTI Adil, reporter and professor at the Royal Naval School in Casablanca.

Mrs. AKNIN Noura, reporter and professor at the Faculty of Sciences of Tetouan.

Mr. FENNAN Abdelhadi, reporter and professor at the Faculty of Science and Technology of Tangier.

Mrs. ELOUAAI Fatiha, examiner and professor at the Faculty of Science and Technology of Tangier.

Thanks to the LIST laboratory that gave me the means to complete this work.

I would like to thank my parents Mohammed & Zineb, my brother Hicham, my sisters Sanae & Fadoua and my wife Aziza who have always encouraged me to achieve this goal. Thank you all for your unconditional love.

Thanks to all my maternal and paternal family who supported me.

Last and not least, I would like to thank all my friends, also my colleagues in the LIST laboratory and Abdelmalek Essaadi University.

Introduction

Motivation

The continued and rapid population growth posed a real problem of accessibility and cost to many vital services in the world. Dealing with this situation was one of the main challenges of the last decades. The most sensitive and vital service was "healthcare". Among the most important objectives that concern the humanity today is to provide quality care to a rapidly growing population while reducing its costs.

A promising application in this field is the development of e-healthcare systems through the accessibility of technology and electronics for the public, which allows people to be constantly monitored. Hospitals equipped with e-healthcare systems help medical and paramedical teams by providing a set of services like the control of devices and facilitating access to medical data used in interdisciplinary communication especially in emergency communications. Constant monitoring enables early detection of emergency and complications of diseases for patients at risk, and provide a wide range of care services for people with varying degrees of cognitive and physical disabilities. Not only the elderly and chronically ill benefit from these systems, but also the children of working parents will also have quality care. The proliferation of mobile ad hoc networks, peer-to-peer communication and wireless sensors devices helped to promote e-healthcare through the development of autonomic computing concepts with potentially a wide range of applications.

The advantage of forming a mobile ad hoc network is to provide wireless com-

munication between heterogeneous devices, anywhere and anytime, without any pre-established communication infrastructure. These devices communicate with other nodes that are in their radio range where each one of them provides services such as message transfer, traffic information, routing, authentication, etc., to form a common network. In addition, the continued evolution of fundamental concepts of ad hoc networks and technological advances of micromechanics, microelectronics, wireless communication and embedded systems have enabled the development of a particular type of ad hoc networks; formed by tiny, multi-functional and low cost nodes. These networks are characterized by their limited resources, commonly known by the LoWPAN networks (Low power Wireless Personal Area Network). This promising technology allows the measurement of physical parameters and transmit data in real time to a base station responsible for the monitoring of a specific area. The low cost, ease of deployment, mobility capacity, adapting to any situation, self-organization, self-recovery and the resiliency ability at any time make it the preferred technology for e-healthcare applications. Many situations can be cited as the coordination of rescue operations in areas without operational infrastructure, monitoring the health status of individuals at risk, monitoring of the activities of daily living, etc.

The constant evolution of networks do not stop there; the latest trend was connect these LoWPAN networks to the Internet, which gave birth to the Internet of Things (IoT) concept. The first LoWPAN networks supported on the terminal nodes just collect data from their physical environment and send it to the base station. Now, this terminal node could be an IP node accessible via the Internet and manageable remotely anywhere and anytime. The transition today from old LoWPAN systems to the Internet of Things and extending the boundaries of the Internet to sensor nodes was thanks to the 6LoWPAN technology (IPv6 over LoWPAN). Instead of ending at the base station level, Internet protocols can now move between two end nodes, which are now able to participate in peer-to-peer communication with all remote peers via the Internet. This will give another dimension to the e-healthcare applications in terms of the ability to monitor and control remotely the sensors and actuators devices.

However, 6LoWPAN networks are faced with high constraints due to their limited resources such as energy, processor, storage, memory, and bandwidth. In addition, many applications require the nodes to be deployed in inaccessible areas, making manual control and individual monitoring of these devices very difficult.

The inherent vulnerability of 6LoWPAN networks, which are generally more prone to physical security threats, add new security challenges. The ability to eavesdrop data, launching a denial of service attack and identity theft are easier to execute in these wireless networks, in addition to other threats because of their integration into the Internet. Unfortunately, security solutions used to protect traditional networks are not valid because of the LoWPAN networks atypical features. In addition to their inherent vulnerability, other threats must be considered such as internal attacks by malicious nodes. Many of these attacks are difficult to detect because of their asymptomatic behavior towards the legitimate processes of the network. Looking at the sensitivity of the potential applications of 6LoWPAN networks in the e-healthcare field that are closely related to the physical world and even to individuals, large-scale deployment of this technology will greatly depend on their performance. In particular, security seems to be a difficult problem because of resource constraints surrounding their design.

This limitation is problematic for a variety of nodes, which is in the scenarios of IoT accurately present constraints of computational capacity and battery power. These nodes are involved in end-to-end transactions with remote peers. Any configuration of a secure channel by establishing security keys, can be prohibitively too expensive for these nodes. For this, a key establishment operation that occurs in effect at the beginning of each new communication without affecting long-short performance is required. For example, a long period of the order of a few seconds or tens of seconds to set up a key, would be acceptable if it is produced only once a day; something that is not valid in the e-healthcare applications that require several exchanges of information in a short time.

Normally, the defense system uses cryptographic mechanisms to secure the data exchanged and prevent or eliminate foreign devices to join the network. These techniques, however, are not effective in protecting against internal threats. For

example, when the nodes are compromised and become attackers, cryptographic techniques cannot detect them and launch various attacks like Denial of Service. Therefore, 6LoWPAN needs an intrusion detection system to monitor any deficiencies in the operation of the network.

The consequences of energy consumption are usually the most critical. The 6LoWPAN nodes powered by low-power battery can be placed in inaccessible locations, where some are integrated into various devices and must have at least the same lifetime as their hosts. The frequent change of battery could be demanding and unacceptable. We must not forget the impact on other neighboring nodes, which can be completely detached from the infrastructure if the default route passes through a node whose battery is exhausted.

Contributions

In this sense, our work has emerged, focusing on two areas of research that show the boundaries of contemporary research in the domain of security of networks with limited resources; that is the area of cryptography key management systems and the field of intrusion detection systems. The main goal of our contribution is to secure the e-healthcare applications in the world of the Internet of Things, protecting data confidentiality and ensuring system availability while minimizing energy consumption. In this work, we propose a security solution using a system based on two lines of defense.

The first line of defense is the security of data exchanged in 6LoWPAN networks by proposing a new key management system. This research emerges when modern cryptography is seen limited in its implementation in systems with resource constraints (memory, CPU, storage, etc.). We considered especially 6LoWPAN networks that are characterized by very limited resources in terms of energy, memory, and bandwidth. These strong constraints require a new understanding of security. Indeed, given the sensitivity of the applications of e-healthcare, deployment of large-scale 6LoWPAN networks through the Internet depends on the reliability of this technology. In particular, the security of these systems is a very difficult

problem to manage because of their limited resources.

An essential functional component of the communication architecture through the secure subsystem is the management of cryptographic keys. This subsystem is of a particular importance in 6LoWPAN networks. The main issue that has been treated is the management of key establishment systems in these networks, which have been proposed as a new approach to the key distribution solution. Our approach is based on unique key pairs so that the compromise of some nodes do not endanger the entire network.

The solution we proposed is based on the pre-deterministic and scalable distribution of these keys as well as improving the resilience of the subsystem of their management without incurring significant additional costs. It is based on self-generation symmetric keys without using the mechanisms of the "master key". It was shown that this method ensures in the same time internal communications between nodes in the same network and external communications between an internal node and an external IP host, without additional cost of key storage. Thus, our approach uses light and strong authentication mechanisms.

We analyzed the security properties of our solution and evaluated its performance through simulations. The results of this analysis have proven the effectiveness of our key management approach and show that it is secure, flexible and adapted to mobility without incurring significant additional costs in terms of energy or storage.

The second line of defense is the intrusion detection system. This solution imposes itself when the security mechanisms based on cryptography reach their limits in relation to the attacks of internal nodes that can hold these mechanisms. Indeed, cryptographic solutions do not support protection against malicious process based on a false behavior that does not disrupt communication protocols. These attacks are based on what is known malicious behavior with regard to the legitimate system, making the diagnosis of an attack of this kind very difficult to rely using only the cryptographic systems tools. These threats require an intrusion detection system adapted to the constraints of 6LoWPAN networks.

We started our investigation by analyzing the existing models for resource con-

strained networks. We became interested in models based on the monitoring of the neighbor-behavior because they are characterized by their ability to adapt to any environment and tolerate the supervision of an encrypted network. Our results led us to propose an approach based on the normal distribution and collaboration between network nodes. It relies on the help of a set of agents for the propagation of all security alerts. We have demonstrated that our optimized intrusion detection model is more energy efficient than existing models. Our model requires no special infrastructure, it is in perfect harmony with the variable nature of connectivity in e-healthcare systems. We have also demonstrated that it reduce the rate of false alarms in the network in a remarkable way and offers a high detection rate.

In our security solution for the Internet of e-healthcare Things, we explored the coupling of cryptography and intrusion detection systems to protect e-healthcare applications based on 6LoWPAN network against malicious attacks difficult to counter by one system. To be exhaustive, the proposed solution must be validated in terms of both security and performance.

Objectives and challenges

The main objective of this thesis is to develop a security system for 6LoWPAN networks applied to e-healthcare systems in the context of the Internet of Things. This objective includes the following challenges that must be specifically addressed:

- Analysis of security needs in the area of e-healthcare that is based on the implementation of the 6LoWPAN technology.
- Study of the state of art regarding security solutions available for the resource-constrained networks and the study of their usefulness in 6LoWPANs networks.
- Design of a security system that meets the constraints and characteristics of 6LoWPAN networks in an e-healthcare system in an Internet of Things heterogeneous environment.

- Adjust the security system to the existing 6LoWPAN protocols to optimize the processing mechanisms and to be conform to network operation.
- Create a basic system that applies to both internal communication between the same 6LoWPAN network nodes and external communications with other IP network devices over the Internet.
- Maximize system security while minimizing energy consumption.

Thesis structure

This thesis document is organized as follows; the introduction, the state of the art section presented in the first two chapters, the contributions section presented in three chapters and the conclusion.

We begin in Chapter 1 with a review of the challenges brought by the passage of the traditional Internet to the Internet of Things. We have introduced the concept of the Internet of Things and how e-healthcare applications benefit from it. Thus, an introduction to the sensor devices used in our study, their operation and their major constraints.

As we study the 6LoWPAN technology, it was necessary to understand its mechanisms. We have introduced the 6LoWPAN in Chapter 2. Its mechanisms, issues and requirements have been defined. Therefore, we analyze the different solutions that have been proposed to address these challenges.

In Chapter 3, we introduced security for 6LoWPAN networks, we conducted a detailed analysis of all it aspects, objectives, threats, attacks and solutions. Thus, in each section, we have summarized the main requirements that we must face in order to design a security system complies with 6LoWPAN networks for e-healthcare applications.

Chapter 4 presents our first solution that provides the first line of defense; the cryptographic key establishment system. We designed our system to provide a solution for establishing keys in a 6LoWPAN network to ensure its security, taking into account the performance requirements such as energy optimization, scalabil-

ity, flexibility, mobility and connectivity. We also provide a detailed evaluation of the results from the point of view of security and energy consumption, which proves the effectiveness of our proposed approach.

Chapter 5 presents the second solution; the second line of defense, the intrusion detection system (IDS). Its main objective is to detect misconduct malicious node and alarms the base station. The results show that the proposed system is able to withstand attacks with efficiency and with less energy consumption.

Introduction

Motivation

La croissance démographique continue et rapide a posé un vrai problème d'accessibilité et de cout à de nombreux services vitaux au monde. Faire face à cette situation était un des principaux défis des dernières décennies. Le service le plus sensible et vital était la santé.

Parmi les objectifs les plus importants qui préoccupent le monde actuellement est de fournir des soins de qualité à une population en croissance rapide tout en réduisant leurs coûts.

Une application prometteuse dans ce domaine est la création des systèmes d'e-santé grâce à l'accessibilité de la technologie et de l'électronique au grand public, qui permet à la population d'être constamment surveillés. Les hôpitaux équipés par les systèmes d'e-santé aident les équipes médicale et paramédicale en fournissant un ensemble de services tel ; le contrôle des appareils, faciliter l'accès aux données médicales, servir dans les communications interdisciplinaires et surtout dans les communications d'urgence. Une surveillance constante permettra la détection précoce des situations d'urgence et les complications de certaines maladies pour les patients à risque, et fournir une large gamme de services de soins pour les personnes avec des degrés de déficience cognitive et physique. Non seulement les personnes âgées et les malades chroniques bénéficieront de ces systèmes, mais aussi les enfants dont les parents travaillent auront aussi des soins de qualité. La prolifération des réseaux mobiles ad hoc, le peer-to-peer et les capteurs sans fil, a

aidé à la promotion de l'e-santé par le développement de concepts de l'informatique autonome avec potentiellement une large gamme d'applications.

L'avantage de former un réseau mobile ad hoc est de fournir une communication sans fil entre des appareils hétérogènes, partout et à tout moment, sans aucune infrastructure de communication préétablie. Ces appareils communiquent avec d'autres nœuds qui sont à leur portée de radio où chaqu'un d'eux fournit des services tels que le transfert de messages, les informations de signalisation, le routage, l'authentification, etc., afin de former un réseau commun. En outre, l'évolution continue des concepts fondateurs de réseaux ad hoc et les progrès technologiques de la micromécanique, la microélectronique, des communications sans fil et des systèmes embarqués ont permis le développement d'un type particulier de réseaux ad hoc; formé par des nœuds minuscules, multifonctionnels et de faible cout. Ces nœuds sont caractérisés par leurs ressources limitées, communément connu par les réseaux « LoWPAN » (réseau personnel sans fil à faible puissance, de l'anglais « Low power Wireless Personal Area Network »). Cette technologie prometteuse permet la mesure des paramètres physiques de son environnement ainsi que la collecte de ces données et leur transmission en temps réel à une station de base responsable de la surveillance d'une zone spécifique. Le faible coût, la facilité de déploiement, la capacité de mobilité, l'adaptation à toutes les situations, l'auto-organisation et l'auto-récupération, et la possibilité de résilience à tout moment font de cette technologie la préférée pour les applications d'e-santé. Nombreuses situations peuvent être citées telles la coordination des opérations de sauvetage dans les zones sans infrastructure opérationnelle, la localisation et la surveillance de l'état de santé de sujet à risque, le suivi des activités de la vie quotidienne, etc.

L'évolution constante des réseaux ne s'arrête pas là ; la dernière tendance était de connecter ces réseaux LoWPAN à l'Internet, ce qui a donné naissance à l'Internet des objets (IdO). Les premiers réseaux LoWPAN pris en charge sur les nœuds terminaux recueillent les données de leur environnement physique et les livrent à une machine centrale appelée station de base. Maintenant, ce nœud terminal pourrait être un nœud IP accessible et gérable à distance, partout et à tout moment. La transition d'aujourd'hui à partir de vieux systèmes LoWPAN vers l'Internet des

objets et l'extension des limites de l'Internet aux nœuds capteurs était grâce à la technologie 6LoWPAN (IPv6 à travers le LoWPAN). Au lieu de s'arrêter à la station de base, les protocoles Internet peuvent maintenant se déplacer entre deux nœuds finaux, lesquels sont maintenant en mesure de participer à des communications bidirectionnelles peer-to-peer avec tous les pairs à distance via l'Internet. Cela donnera une autre dimension aux applications de l'e-santé en matière de la capacité de surveiller et de contrôler les appareils capteurs et actuateurs à distance.

Cependant, les réseaux 6LoWPANs sont confrontés à des contraintes élevées en raison de la limitation des ressources telles que l'énergie, le processeur, la capacité de stockage, la mémoire et la bande passante. En outre, de nombreuses applications nécessitent le déploiement de nœuds dans les zones inaccessibles, ce qui rend le contrôle manuel et un suivi individuel de ces dispositifs très difficile.

La vulnérabilité inhérente des réseaux 6LoWPAN, qui sont généralement plus enclins à des menaces de sécurité physiques, rajoute de nouveaux défis de sécurité. La capacité d'espionner les données, le déni de service et le vol d'identité sont plus faciles à exécuter dans ces réseaux sans fil et sans infrastructure, en plus d'autres menaces qui s'ajoutent en raison de leur intégration dans l'Internet. En outre, les solutions de sécurité utilisées pour protéger les réseaux traditionnels ne sont pas valables en raison des caractéristiques atypiques de réseaux LoWPAN. En plus de leur vulnérabilité inhérente, des nouvelles menaces sont rajoutées, telles que les attaques internes par des nœuds malveillants. Beaucoup de ces attaques sont difficiles à détecter et contrecarrer en raison de leur comportement asymptomatique vis-à-vis des processus légitimes du réseau. Le compte tenu de la sensibilité des applications potentielles des réseaux 6LoWPAN dans le domaine de l'e-santé qui sont étroitement liés au monde physique et même à des individus, un déploiement à grande échelle de cette technologie dépendra beaucoup de leur performance. En particulier, la sécurité semble être un problème difficile en raison des contraintes de ressources qui entourent leur conception.

Cette limitation est problématique pour une variété de nœuds, ce qui est dans les scénarios de l'IdO présentent précisément des contraintes liées à la capacité de calcul et à la puissance de la batterie. Ces nœuds sont impliqués dans des transac-

tions de bout en bout avec des pairs à distance. En outre, toute configuration d'un canal sécurisé par l'établissement des clés de sécurité, peut être prohibitif, trop cher pour ces nœuds. Pour cela, une opération d'établissement de clé qui se produit en vigueur au début de chaque nouvelle communication sans affecter à long court les performances est exigée. Par exemple, une longue phase de l'ordre de quelques secondes ou dizaines de seconds pour paramétrer une clé, serait acceptable si elle n'est produite qu'une seule fois par jour ; chose qui n'est pas valable dans les applications d'e-santé qui nécessitent plusieurs échanges d'informations en un temps court.

Normalement, le système de défense utilise des mécanismes cryptographiques pour sécuriser les données échangées et prévenir ou éliminer les appareils étrangers à rejoindre le réseau. Ces techniques, cependant, ne sont pas efficaces lors de la protection contre les menaces internes. Par exemple, lorsque les nœuds sont compromis et deviennent des attaquants, les techniques cryptographiques ne peuvent pas les détecter. Ils peuvent lancer diverses attaques, entre-autres les attaques par déni de service. Par conséquent, 6LoWPAN a besoin d'un système de détection d'intrusion pour surveiller toute anomalie touchant au fonctionnement du réseau.

Les conséquences liées à la consommation d'énergie sont généralement les plus critiques. Les nœuds 6LoWPAN alimenté par la batterie de faible puissance peuvent être placés dans des endroits inaccessibles, où certains sont intégrés dans des appareils divers et doivent avoir au moins la même durée de vie que leurs hôtes. La modification fréquente d'une batterie pourrait être exigeante et inacceptable. Il ne faut pas oublier le retentissement sur les autres nœuds voisins, qui peuvent être totalement détaché de l'infrastructure si la route par défaut passe par un nœud dont la batterie est épuisée.

Contributions

Dans ce sens, notre travail a émergé, en se focalisant sur deux domaines de recherche qui présentent les limites de la recherche contemporaine dans le volet de la sécurité des réseaux avec ressources limitées ; qui sont le domaine des systèmes de ges-

tion des clés de cryptographie et le domaine des systèmes de détection d'intrusion. L'objectif principal de notre contribution est de sécuriser les applications d'e-santé dans le monde de l'Internet des Objets, en protégeant la confidentialité des données et en assurant la disponibilité du système, toute en minimisant la consommation de l'énergie. Dans ce travail nous proposons une solution de sécurité à l'aide d'un système basé sur deux lignes de défense.

La première ligne de défense est la sécurité des données échangées dans les réseaux avec fortes contraintes de ressources notamment dans les réseaux 6LoWPANs. Cette recherche émerge lorsque la cryptographie moderne se voit limité dans sa mise en œuvre dans les systèmes avec contraintes de ressources (mémoire, processeur, espace de stockage, etc.). Nous avons considéré en particulier les réseaux 6LoWPAN qui sont caractérisées par des ressources très limitées en termes d'énergie, de mémoire et de bande passante. Ces fortes contraintes nécessitent une nouvelle compréhension de la sécurité. En effet, compte tenu de la sensibilité des applications de l'e-santé, un déploiement des réseaux 6LoWPAN à grande échelle à travers l'Internet dépend de la fiabilité de cette technologie. En particulier, la sécurité de ces systèmes est un problème très difficile à gérer en raison de ressources limitées.

Un composant fonctionnel essentiel de l'architecture de communication à travers le sous-système sécurisé est la gestion des clés de cryptographie. Ce sous-système a une importance particulière dans les réseaux 6LoWPAN. La principale problématique qu'on a traitée est la gestion des systèmes d'établissement de clés dans ces réseaux, où on a proposé comme solution une nouvelle approche du développement et de la distribution des clés. Notre approche est basée sur des clés paires uniques afin que le compromis de certains nœuds ne mette pas en danger l'ensemble du réseau.

La solution qu'on a proposée est basée sur la distribution pré-déterministe et évolutive de ces clés ainsi que l'amélioration de la résilience du sous-système de leur gestion sans induire des coûts supplémentaires importants. Elle est fondée sur l'auto-génération des clés symétriques sans avoir recours aux mécanismes de la « clé maîtresse ». On a montré que cette technique permet d'assurer au même temps les communications internes entre les nœuds du même réseau et les com-

munications externes entre un nœud interne et une hôte IP externe, sans un coût supplémentaire de stockage des clés. Ainsi, notre approche utilise des mécanismes d'authentification légers et efficaces. Nous avons analysé les propriétés de sécurité de notre solution et évalué sa performance à travers des simulations. Les résultats de cette analyse ont prouvé l'efficacité de notre approche de gestion des clés et ont démontré que c'est sécurisé, souple et adapté à la mobilité, sans encourir des coûts supplémentaires importants en termes d'énergie ou de stockage.

La seconde ligne de défense est le système de détection d'intrusion. Cette recherche émerge lorsque les mécanismes de sécurité reposant sur la cryptographie atteignent leur limite par rapport aux attaques des nœuds internes qui peuvent détenir ces mécanismes. En effet, les solutions cryptographiques ne gèrent pas la protection contre les processus malveillants basée sur un faux comportement qui ne perturbent pas les protocoles de communication. Ces attaques sont basées sur ce qu'on appelle un comportement malveillant à l'égard du système légitime, ce qui rend le diagnostic d'une attaque de ce genre très difficile de se fier uniquement sur les outils des systèmes cryptographiques. Ces menaces nécessitent un système de détection d'intrusion adaptée aux contraintes des réseaux 6LoWPAN.

On a commencé notre enquête en analysant les modèles existants pour les réseaux avec des contraintes de ressources. On s'est intéressé aux modèles basés sur le suivi du comportement du voisin parce qu'ils sont caractérisés par leur capacité à s'adapter à n'importe quel environnement et à tolérer la surveillance d'un réseau crypté. Nos résultats nous ont conduits à proposer une approche basée sur la distribution normale et la collaboration entre les nœuds du réseau. Elle s'appuie sur la collaboration d'un ensemble d'agents pour la propagation de toutes les alertes de sécurité. Nous avons démontré que notre modèle de détection d'intrusion optimisé est plus économe en énergie que les modèles existants. Notre modèle ne nécessite pas d'infrastructure particulière, il est en parfaite harmonie avec la nature variable de la connectivité dans les systèmes d'e-santé. Nous avons également démontré qu'il réduit le taux de fausses alarmes dans le réseau d'une manière remarquable et offre un taux de détection élevé.

Dans notre solution, nous avons exploré le couplage de la cryptographie et de

détection d'intrusion pour protéger les systèmes e-santé basé sur le réseau 6LoWPAN contre toute attaque malveillante difficile à contrecarrer par un seul système. Pour être exhaustive, la solution proposée doit être validée à la fois en termes de sécurité et de performance.

Objectifs et défis

L'objectif principal de cette thèse est de développer un système de sécurité pour les réseaux 6LoWPAN appliquées sur les systèmes d'e-santé, dans le contexte de l'Internet des objets. Cet objectif comprend les défis suivants qui doivent être spécifiquement abordés :

- Analyse des besoins de la sécurité dans le domaine de la santé qui se base sur l'application de la technologie 6LoWPAN.
- Etude de l'état des lieux en matière des solutions de sécurité disponible pour le réseau à faibles ressources et l'étude de leur utilité dans les réseaux 6LoWPANs.
- Conception d'un système de sécurité répondant aux contraintes et caractéristiques des réseaux 6LoWPAN dans un système d'e-santé dans un environnement hétérogène d'Internet des Objets.
- Adapter le système de sécurité aux modes et aux protocoles de 6LoWPAN existantes afin d'optimiser les opérations de traitement et de la rendre conforme à leur fonctionnement.
- Créer un système de base qui s'applique à la fois aux communications internes entre les mêmes nœuds de réseau 6LoWPAN et aux communications externes avec d'autres périphériques réseau IP à travers Internet.
- Maximiser la sécurité du système tout en minimisant la consommation d'énergie.

Structure de la thèse

Ce document de thèse est organisé comme suit; d'abord l'introduction puis l'état de l'art a été présenté dans les deux premiers chapitres et les contributions ont été présentées en trois chapitres avant de conclure.

Nous avons commencé au 1er chapitre par un examen des défis posés par le passage de l'Internet traditionnel à l'Internet des Objets. Nous avons introduit le concept de l'Internet des Objets et son apport dans les applications de l'e-santé. Ainsi, une introduction aux appareils capteurs utilisés dans notre étude, leur fonctionnement et leurs limites.

Puisque nous étudions la technologie 6LoWPAN, il était nécessaire de comprendre ses mécanismes. Dans le deuxième chapitre Nous avons introduit le 6LoWPAN et on a définit ses mécanismes de fonctionnement, les enjeux ainsi que les besoins. Par conséquent, nous avons analysé les différentes solutions qui ont été proposées pour relever ces défis.

Dans le 3ème chapitre, nous avons entamé la sécurité pour les réseaux 6LoWPAN, nous avons mené une analyse détaillée de tous les aspects informatiques, les objectifs, les menaces, les attaques et les solutions. Ainsi, dans chaque section, nous avons résumé les principales exigences que nous devons traiter afin de concevoir un système de sécurité conforme aux réseaux 6LoWPAN pour les applications d'e-santé.

Le 4ème chapitre présente notre première solution qui fournit la première ligne de défense; le système d'établissement de clé cryptographique. Nous avons conçu notre système pour fournir une solution par l'établissement de clés dans un réseau 6LoWPAN afin assurer sa sécurité, en tenant compte des exigences de performance telles que l'optimisation de l'énergie, l'évolutivité, la flexibilité, la mobilité et la connectivité. Nous avons fourni également une évaluation détaillée des résultats du point de vue de la sécurité et de la consommation d'énergie, ce qui prouve l'efficacité de notre approche proposée.

Le 5ème chapitre présente la seconde solution et la deuxième ligne de défense; le système de détection d'intrusion (IDS). Son principal objectif est de détecter

les nœuds malveillants et d'alerter la station de base. Les résultats montrent que le système proposé est capable de résister à des attaques avec efficacité et avec moindre consommation d'énergie.

When it comes to health, your zip code (postal code) matters more than your genetic code.

Dr. Tony Iton

1

E-healthcare in the Internet of Things

In the Internet of Things, devices collect and share information with each other directly through the internet, which is used to store and analyze data quickly, in real time and with a good precision. This will offer many interesting opportunities across several areas; like industrial and structural monitoring, environmental monitoring, vehicle telematics, home automation, etc. But nowhere the Internet of Things offers greater promise than in the field of e-healthcare, where its principles are already applied to improve access to care, improve its quality and reduce its costs. Although significant benefits, the Internet of e-haltcare Things filed still has major challenges that are addressed in this document.

1.1 Internet of Things

1.1.1 Concept

The evolution of the Internet of Things from a concept to a reality is considered as a big challenge for the combined scientific and technical teams that work on the development of the Internet [1]. It is an opportunity for those interested in technology and its employees as companies and developers, and all the rest of the other sectors in which will be used in order to develop their services and their products. The number of embedded devices with IP is growing ascending continuously. It is expected to reach the 50 billion device by 2020 [2], due to the evolution in the electronics sector, processors, transmitters, communication component, and batteries, etc., what makes it easy to incorporate into many applications and machines, and even the invention of new ones that could not have been created by the past circumstances before this development. The first objective of creating the Internet of Things and the development of its mechanisms is to make the devices more autonomous and independent from the direct control of the human user, and to allow this latter tracking and remote control these devices, each according to its field. The remaining end of this evolution is to get more facilities and greater possibilities in making decisions. With the sensors, it became possible to obtain information and data directly from the physical world. Thanks to IP, they can be accessed from anywhere in the world in the real time, which give the opportunity to create intelligent devices (smart sensors). The collected data is used to make better and faster decisions. Sensors can now communicate with the other devices, surrounding it or in a distant, in order to exchange the necessary information.

The main force of the idea of the Internet of Things is the huge impact that will have on several aspects of the daily life and the behavior of potential users (fig. 1.1.1 [3]). From the perspective of a private user, the most obvious effects of the use of the Internet of Things will be visible to both domestic and work domains. In this context, home automation, assisted living, e-healthcare, improving learning are just a few examples of possible scenarios of application in which the new model

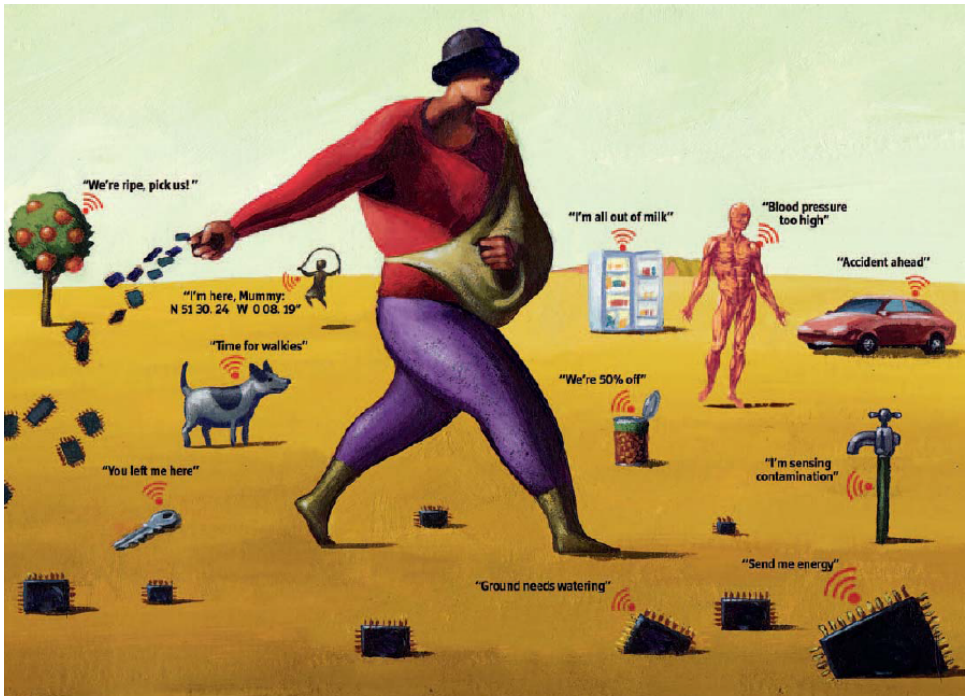

Figure 1.1.1: A description of the vision of Internet of Things.

will play a leading role in the near future. Thus, from the perspective of business users, the most interesting consequences will also be visible in areas such as industrial manufacturing, automation, logistics, business and process management, and transportation of people and goods.

The Internet of Things goes well beyond. Some examples of things that could be considered part of the Internet of Things are the connected devices. As there are refrigerators, ovens and washing machines that can be controlled from a smartphone via the Internet connection [4]. It is only the first step of what is to come. At the personal and professional level, the Internet of Things could change the world as we know it today (fig. 1.1.2 [5]). Consider some of the applications that could take place. A farmer must know at all times the conditions of the field he develops. His job is to check the temperature and humidity of the field regularly and record this information on a computer. But suppose all these data were monitored and recorded automatically in an online service, so that the farmer has information of how the area is growing remotely and may even know how it is in real time. And there's more, with fairly cheap sensors, he absolutely could monitor all plants that grow, how they grow and if they have problems.

Domestic applications could be equally important. For example, we could have sensors and controllers in different parts of the house. If we go on a trip and we are not be sure if we removed the heat of the kitchen, or shutters, windows or lights are left as desired. Everything would be as simple as accessing the service that we control our home, not just to check that everything is fine, but also change their status. Or, contrariwise, back in a few hours at home, you can even schedule when you want to start preparing food [6]. Things like regulating the temperature of our house when we are there or turn on lights automatically, could be made of everyday life. It is the Internet of Things, the things that surround us, that would be permanently connected.

However, many difficult issues remain to be addressed and both social and technological problems must be settled before the Internet of Things idea being widely accepted, especially with regard to embedded and resource constraints devices.

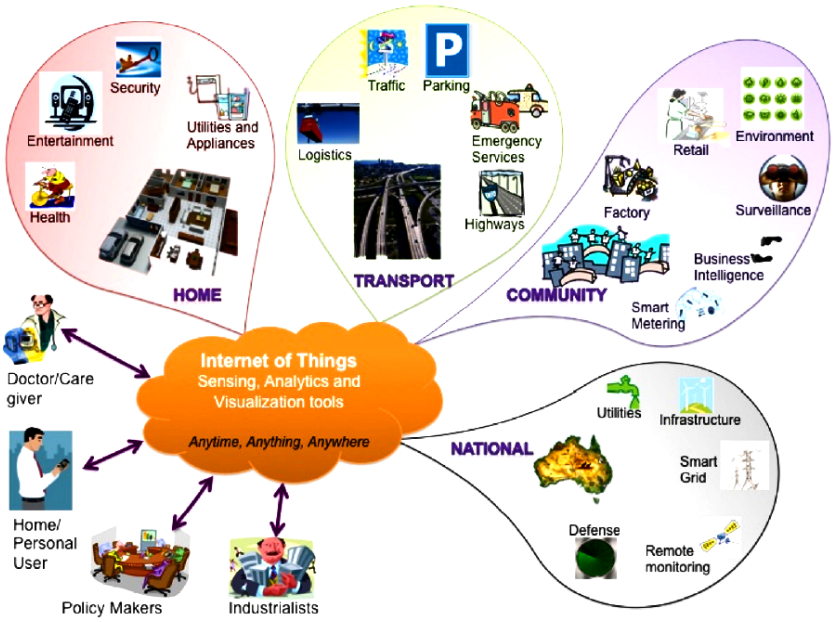

Figure 1.1.2: Applications areas in the Internet of Things.

Central questions are complete interoperability of possible interconnected devices, providing an ever-higher degree of resourcefulness, allowing their adaptation and autonomous behavior while ensuring trust, privacy and security. Therefore, the Internet of Things idea poses several new problems regarding aspects of networking. Actually, the things that compose the Internet of Things will be characterized by low resources in terms of computation and energy capacity. Therefore, solutions should pay particular attention to resource efficiency, besides the obvious scalability problems.

1.1.2 Standardization

The Internet is among the largest and most important inventions of the last half century, which radically changed the lives of human beings and was able to touch all sectors and all the society groups [7]. From an academic network connecting some computers (1969) to the global network used by nearly 3 billion users (2014), approximately 40 percent of the earth's population [8], moving from a

network of computers used by human users, to a network connecting everything at any time in any place. Radical changes happen in the current Internet transform it to a network of interconnected devices that not only sense information from the environment and control the physical world, but also use Internet standards to provide many services using different applications. The Internet of Things is about to transform the actual static Internet into a fully integrated Future Internet [9]. The Internet revolution has led to the interconnection between people from and in different places. The next revolution will be the interconnection between the objects to create an intelligent environment. Only in 2008, the number of interconnected devices on the planet does exceed the actual number of people. Currently, there are 25 billion interconnected objects and should reach 50 billion objects by 2020 (fig. 1.1.3 [2]).

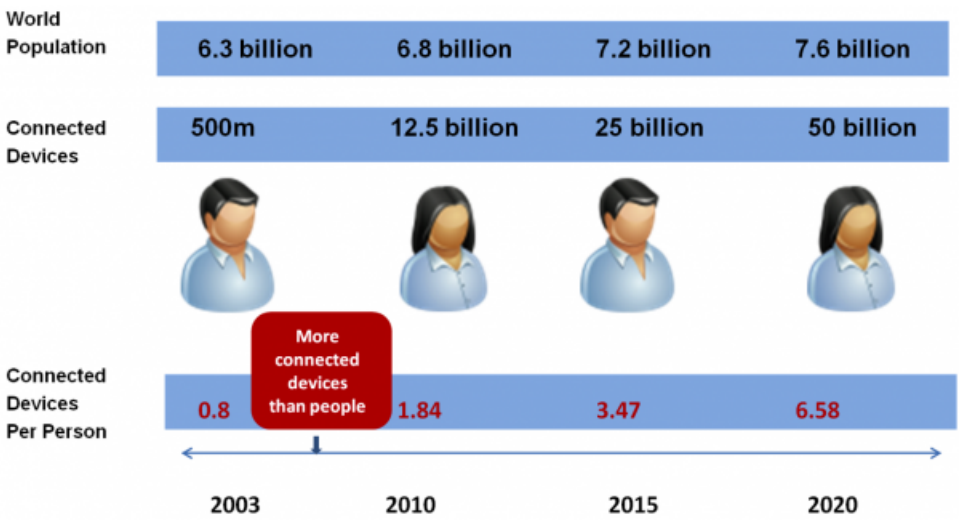

Figure 1.1.3: The number of connected devices evolution.

The term of Internet of Things appeared for the first time in a project of a framework of the "supply chain management" in 1999 [10]. Its definition was changed within the evolution of technology, but the goal remains the main: facilitating and enabling the remote use of sensed information without the help of human intervention. The current form of the concept of Internet of Things is to create a net-

work of "things" connected via the Internet, which combines information from their environment and interact with the physical world. However, we can consider the birth year of the Internet of Things is the 2008, as in this year it was its recognition by the European Union (EU) where the First European Internet of Things conference was organized [11]. In addition, a group of international companies launched the IPSO Alliance (Internet Protocol for the networking of Smart Objects) [12] to enable the Internet of Things and to promote the use of Internet Protocol (IP) in "smart objects". The IPSO alliance now consist over 50 member companies, including Cisco, Ericsson, Bosch, Fujitsu, SAP, Intel, Sun and Google.

The Institute of Electrical and Electronics Engineers (IEEE) [13] embarked on an a project that aim to build a global architecture for the Internet of Things for a multitude of industries and technologies. P2413 working group [14], whose engineers working on the issue since July 2014, and want to form a framework for interoperability among connected objects and related applications in industrial monitoring, home automation, traffic monitoring, e-healthcare and all other sectors likely to use the Internet of Things in the near future. The standard would allow data sharing between Internet of Things systems. The P2413 group hopes laid the first stones of such systems that may be common to different industries, with the aim of reaching a standard finalized by 2016 [15], in coordination with other organizations, including the European Telecommunications Standards Institute (ETSI) [16], the International Organization for Standardization (ISO) [17] and Machine-to-Machine (M2M) group [18] is part of the plan of P2413 group. Currently, 23 vendors and organizations are represented in this group like Cisco, Oracle, Huawei, Qualcomm, General Electric, and the ZigBee Alliance.

The open nature of the Internet and that no one, or a specific destination owned it, allowed for many actors from academics researchers, companies and organizations, in a formal or in an informal sector, to enrich it with new ideas and recent developments, made it fertile ground and vital to scientific and technical research. A set of protocols work together in order to serve Internet and make it applicable, these protocols are in a permanent and ongoing development, evolving development of the technology and come to meet the users' needs, whatever its use,

whether professional or recreational (fig. 1.1.4 [19]). Among the most important these protocols, which have been linked closely connected to the Internet, is the IP protocol (Internet protocol) [20]. It allows each device connect the Internet by providing it an address that can determine its position within the network containing millions of devices and allows the transfer of data packets between devices through the routing protocols.

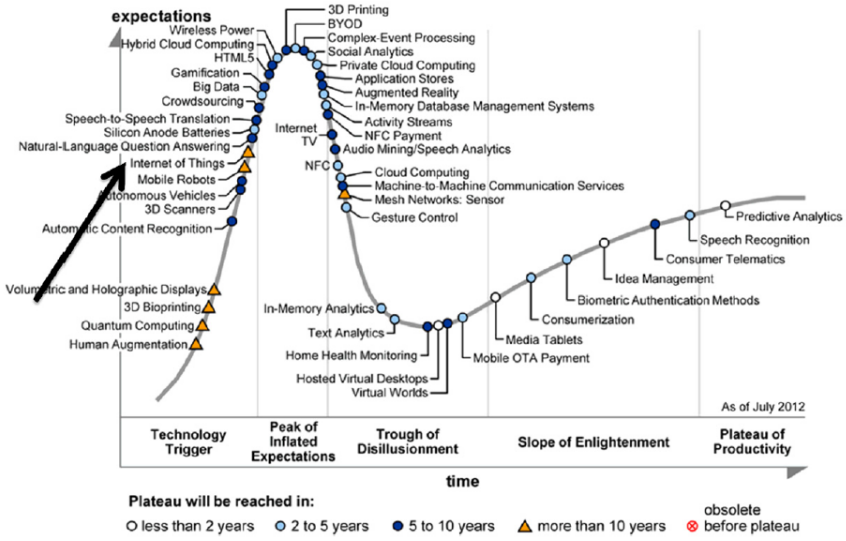

Figure 1.1.4: The Internet of Things within the emerging technologies.

Currently, the Internet is composed of two major groups of layers, the first layer form the infrastructure consisting of intermediary devices, routers, and wired and wireless links, as well as servers and data centers. The second layer formed by the computers, phones, tablets, printers and all machines used directly by human users, which constitute the boundaries of the online world.

The Internet of things will bring the online world to the physical world and makes it an integral part of it. It will eliminate all boundaries making everything and everyone linked directly to the Internet (fig. 1.1.5 [21]). It consists of devices authorized to use the IP; including sensors, RFIDs (Radio Frequency IDentification), etc. While the use of Internet had been calculated previously using the num-

ber of humans users onwards. Now, it will be accounted calculating the number of devices connected to the Internet, which are expected to reach the millions in the coming years, as it can be incorporated anywhere and anything, does not consume a lot of energy, has the ability to communicate wirelessly, and there are many of these devices currently in use but lacking the IP protocol. This what form a challenge from among many challenges, as the IP protocol had been designed agree to ordinary devices like computers and servers, which does not approve resource-constrained devices like sensors.

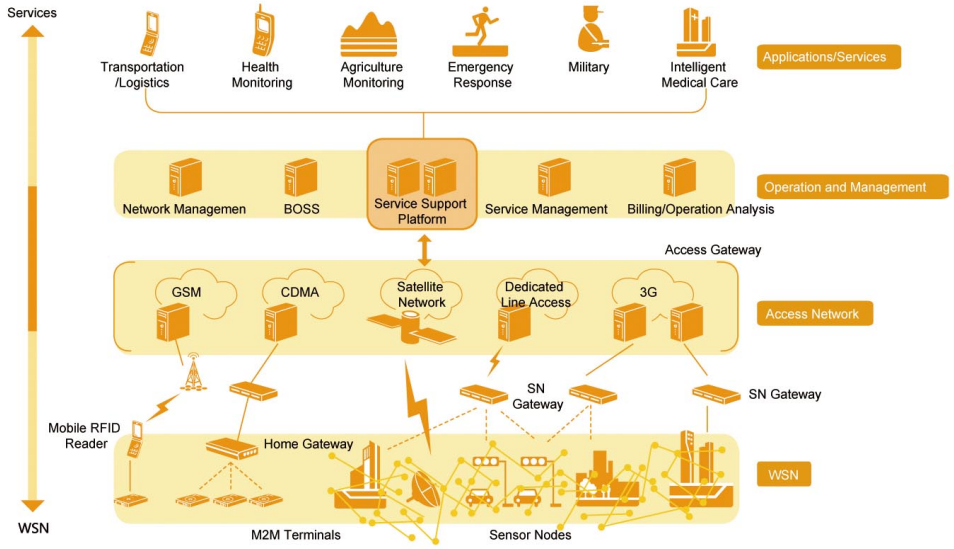

Figure 1.1.5: Framework of The Internet of Things services.

Supply these devices with limited resources with IP is an important step that will enable the realization of the concept of Internet of Things in the real world. Even though it constitutes a sub-group within other projects that involve the concept of the wide Internet of Things concept, but it is considered the most challenging one as it opens the door to many issues to be solved, and one of the main groups that will allow the Internet of Things becomes real.

In order to enable these devices connecting to the Internet, and make the concept of Internet of Things a reality, the Internet Engineering Task Force (IETF)

[22] developed the 6LoWPAN technology; (IPv6 over Low power Wireless Personal Area Networks), one of the most important technologies that enable the resource-constrained devices to get an IP address. The first 6LoWPAN specifications and guidelines was published in 2007 and it reaches its objectives current this year (2014) [23]. 6LoWPAN presents the subject of our study where we will try through what follows, define it and give an overview of the techniques that it uses, as well as the challenges faced in order to activate it in the sensors devices and make it functional and practical.

Before talking about 6LoWPAN, we must differentiate between the terms of "6LoWPAN" and "LoWPAN". 6LoWPAN meaning brings us to the set of technologies and standards that enable IPv6 over low power networks. Whilst the "LoWPAN" means any network with low power and related nodes with limited resources, like Wireless Sensors Networks.

1.1.3 Internet of Things in the service of e-healthcare

Medical e-healthcare applications in the Internet of Things, especially the sensors networks, are designed to improve existing health services and remote monitoring especially for people with difficulties such as patients, handicapped, elderly, children and the chronically ill [24]. The benefits obtained with these systems are huge; one of the main advantages is the remote monitoring. Due to the monitoring over the Internet, it will be easy to identify emergency conditions for at-risk patients and people with varying degrees of cognitive and physical disabilities, which will enable them to have a more independent life. Moreover, children and babies will be taken care while their parents are away. Identify real-time emergencies such as heart attacks in a very short time is enough to save the patient's life considering that without these techniques, these conditions will not be identified at all. Especially, if we hold a system that provides both identification and action in real-time. With these systems, the dependence on caregivers and healthcare professionals will be increasingly diminished [25].

Among the advantages is the capability to identify the context of the person

to be monitored and its environment. Context-awareness systems allows caregivers to have continuously an idea of the living conditions and the environments in which monitored persons are. This is occur through systems that incorporate more than one type of sensing capabilities. To get a clearer view of the context, we must merge the information collected by these sensors [26]. Context information is used to detect unusual situation and make accurate and useful inferences about it. For example, during the night, if the monitored person is in the bedroom in a lying position may indicate a normal situation, while lying in the living room in the middle of the day may indicate an alarm condition. Sensitivity to context provides this useful information.

The Internet of Things also provides easier documentation, fast and accurate patient records data are collected, sorted and organized, allowing doctors consult these digitized records without leaving their room. What contributes to save their time, save money for the hospital and allow patients to be seen in a very short time. It also allows patients to consult their health status data in real time, which educate and empower them to control and monitor their health themselves. Moreover, it allow users to track their daily activity of walking, eating and sleeping, which encourage people to improve their health status and fitness, and change their behavior.

Remote monitoring help doctors to monitor many people in their home reducing their risk of hospitalised infections. In the United States, the Federal Communications Commission (FCC) has provided potential cost savings just with using the MBANs sensors (Medical Body Area Network) [27]:

- Thanks to MBAN technology, doctors can intervene before a patient's condition deteriorates seriously; which resulting in less time spent in the intensive care unit, and many cost savings by reducing the number of visits. A healthcare company in the United States estimated at $ 1.5 million per month could be saved only if emergency transfers could be reduced by detecting and treating the health of the patient earlier.

- Sensors can help reduce hospital-acquired infections. The industry believes

that disposable sensors could help save about $ 2 000 to $ 12 000 per patient and $ 11 billion nationwide.

- Just remote monitoring of patients with congestive heart failure could save more than $ 10 billion per year.

1.2 E-healthcare applications

In healthcare, the Internet of Things plays an important role in many applications that may be divided within three areas of intervention: clinical care, remote monitoring and context-awareness [28]. Automating data collection reduces the risk of human error. The caregivers in this case will obtain reliable information about the patient with a negligible error rate. This will improve the quality of diagnosis and will avoid human intervention that may collect or transmit false information, which can have a dangerous impact on patient health (fig. 1.2.1 [29]).

1.2.1 Clinical care

In hospitals, hospitalized patients, especially those with critical cases in intensive care unit, need continuous and close attention to react rather possible in a crisis case, which will give more chance to save patients life. Thanks to IP-based sensors, we can collect remotely the necessary information that has a relationship with the patient health status, and send them through the Internet to caregivers for further review and analysis. This will prevent caregiver's displacement to each patient to check his state, and will save their time for more interventions.

Many health professionals can collaborate to examine the same patient according to each one specialty, just by analyzing the flow of data collected by the sensors. The identification of emergency conditions for at risk patients will become an easy task.

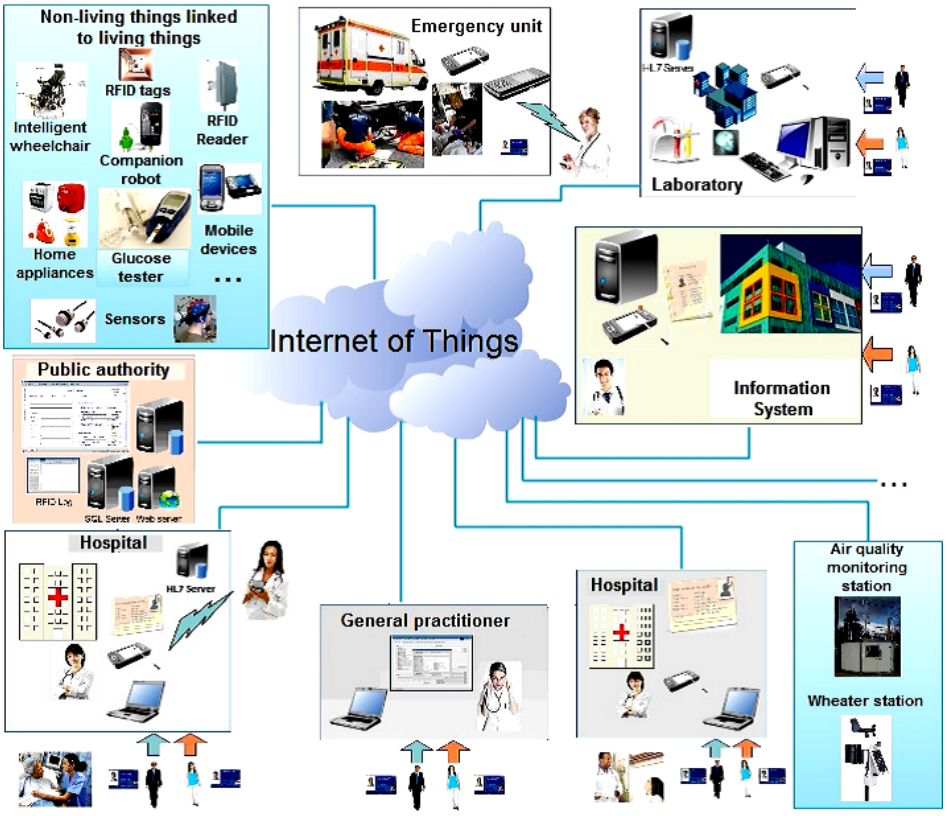

Figure 1.2.1: The e-healthcare fields and applications linked by the Internet of Things.

1.2.2 Home care

We can take advantage of these sensors in the home monitoring for the elderly, handicapped, people with special needs or the owners of chronic diseases such as diabetes, asthma, chronic obstructive pulmonary, congestive heart failure, and memory decline, etc. [30]. They will avoid trouble navigating to the hospital from time to time to check their health state. As they have an unstable condition that may develop to the worse at any moment, the sensors will warn the medical staff remotely in order to intervene. The patient can also use these sensors himself for tracking his health daily, as well as by its family, even remotely via the Internet.

1.2.3 Remote monitoring

Elderly, child or chronically ill need to be examined almost daily, the possibility of a remote monitoring will help them avoid making rounds to the hospital for control. Because of their critical status, sometimes changes in their health goes unnoticed until the disease will be developed to a crisis stage. Remote access sensors will help caregivers to have pre-diagnosis and earlier intervention before things go wrong [31]. Thus, the people with different degrees of cognitive and physical disabilities will be enabled to have a more independent and easy life.

It can be used on a personal level in order to help take daily preventive measures to maintain health. Its connection to internet will enable it to obtain the necessary information and updates in order to help people organize their lives, which fall within the so-called smart devices that interact with the requirements and variables of its owner.

1.2.4 Context-awareness

Having the ability to identify the patient's condition and the environment where he is located, will greatly assist healthcare professionals to understand the variations that can influence the health status of this patient. Because the environment have a very important effect on the health of any person. In addition, the change

of physical state of a patient may increase the percentage of its vulnerability to a disease and be a cause of a health deteriorating.

The use of several types of specialized sensors to capture various information about the patient physical condition: he walks, he sleep, he runs,etc. or about the environment where he is: Wet, hot, cold, etc. and collaboration between them to collect meaningful information, will provide a comprehensive understanding of the context of the patient, as he is hospitalized, at home or anywhere. It will help in emergency cases to well locate the patient and be aware of what type of emergency intervention must be taken.

1.2.5 Monitoring of disasters

Although triage protocols for emergency medical services already exist, their effectiveness can deteriorate rapidly if the number of victims increases. It is necessary to improve the assessment of the health status of first responders of these deadly disasters. The increased portability, scalability and rapid deployment nature of wireless sensing systems can be used to automatically report remotely the levels of many victims and to continuously monitor the health of first responders at the scene of the disaster more effectively.

1.2.6 Example: Continuous cardiac monitoring

Cardiovascular diseases are the leading cause of death worldwide since more than twenty-two million people are affected, this number should triple by 2020 [32]. This requires immense expenses for managing such disease. The looming health crisis attracts researchers and industry to look for optimal and rapid solution to perform cardiac remote monitoring, with medical records updates in real-time via the Internet, by economic solutions valid for the entire world.

A wearable WBAN (Wireless Body Area Network) IP-based sensor is efficient for this mission. It can be placed on specific places of the body of the patient to continuous measure its electrocardiograms signs (ECG) and transmit them to the hospital supervisor medical central unit in real-time [33]. Thus, it can mon-

itor patient under natural physiological states of health in the long term without constraining their normal activities. These sensors are able to gather information from implantable cardiac defibrillators (ICDs) to detect and treat ventricular tachyarrhythmia and prevent sudden cardiac death (SCD).

The following table (Table 1.2.1) gives an overview of some e-healthcare applications divided by the most important studies on this field [28].

1.3 E-healthcare systems

Several devices and systems must work together in the context of the Internet of Things, to contribute to the operation and improvement of the overall healthcare system. End-user healthcare monitoring application need a diverse set of information concerning the supervised person conditions, and the environment where he is located, to get an idea about his health and the type of intervention that must be taken. These information will be collected by a set of sensors of different types, everyone depending on its application.

Most existing solutions include one or more types of sensors worn by the patient, forming a Body Area Network (BAN), and a group of sensors deployed in the environment forming a Personal Area Network (PAN). These two elements are connected to a backbone network via a gateway, which connect them to the Internet. Moreover, a Medical Center Unit (MCU) that collect sensed information, treat it, analyze it and stored in a database. At the application level, the health professionals and other caregivers can monitor health information of the patient in real time via a graphical user interface (GUI) [34]. Emergencies occur alerts by application and such warnings and other information of the state of health of the monitored person can be achieved via mobile devices such as laptops, Personal Digital Assistants (PDAs), tablets and smartphones.

Activity	Applications
Daily activities	AICO
	CareNet Disp.
	Caregiver's Ast.
	WISP
	LiveNet
Movement detection	ITALH
	Act. Mon.
	Fall Det.
	Fall Detection
	Smart Phone HCM
	Smart HCN
	HipGuard
Location tracking	RFID way finding
	Ultra Badge
	ZUPS
	ALMAS
	Passive mon.
Medication intake	RFID medic. ctrl.
	iCabiNET
	iPackage
Medical status monitoring	MobiHealth
	CodeBlue
	AlarmNet
	LifeGuard
	Med. Supervision
	FireLine
	Baby Glove
	LISTENse
	WLAN ECG
	Mobile ECG
	PATHS
	AWARENESS

Table 1.2.1: E-healthcare applications overview.

1.3.1 WBAN (Wireless Body Area Network)

The WBAN [35] is a network of wireless devices that use radio frequencies to communicate. It consists of a set of miniature devices implanted in or around the human body that can act as sensors or actuators in order to monitor vital body parameters (fig. 1.3.1 [36]). They communicate their data wirelessly to a remote service center to alert caregivers in real time in a hospital, a clinic or elsewhere. They are characterized by a large autonomy and using very low power currents.

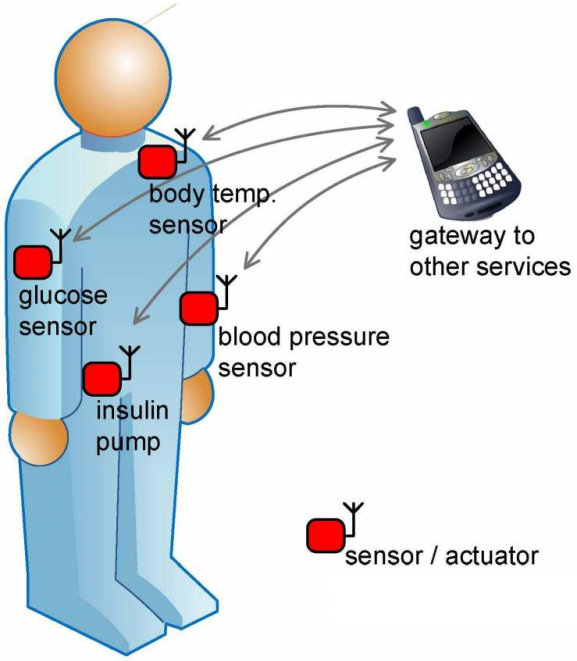

Figure 1.3.1: Wireless Body Area Network schema.

Fig. 1.3.2 shows a typical wearable sensor node for medical applications; the SHIMMER platform [37]. The SHIMMER comprises an embedded microcontroller TI MSP430 with 8-MHz clock speed, 10-KB RAM and 48-KB ROM, and a low-power radio Chipcon CC2420; IEEE 802.15.4 of 2.4 GHz and 250-Kb/s PHY data rate. The total device power budget is approximately 60 mW when active, with a sleep power drain of a few microwatts.

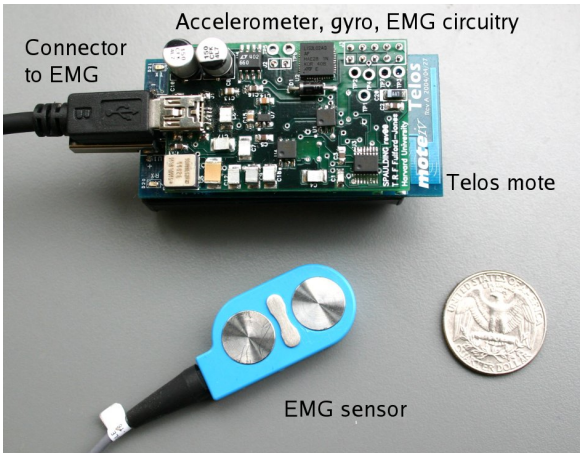

Figure 1.3.2: The SHIMMER wearable sensor platform.

1.3.2 WPAN (Wireless Personnal Area Network)

WPAN [38] is a network of a set of small devices connected wirelessly, characterized by their resource-constrained and a low range. Devices such as video cameras, or sound, pressure, humidity, luminosity, and temperature sensors can be used to monitor the patient environment and provide important information about his context. They are able to communicate with powerful devices to transmit their data. In the context of the Internet of Things, these data can be transmitted and accessed through the Internet.

Fig. 1.3.3 and fig. 1.3.4 show a widely usable wireless sensor platform, the TelosB platform [39]. TelosB is based on the low-power micro-controller MSP430 16-bit with a clock frequency of 4 MHz an 10-KB RAM. It implements the IEEE 802.15.4 transceiver CC2420 with a claimed data rate of 250 Kbps.

1.3.3 Gateway

A gateway system to connect the WBAN and WPAN to internet is essential if we want to have an Internet of Things system. This gateway will play the role of linking the ad hoc devices with surveillance machines consulted by caregivers.

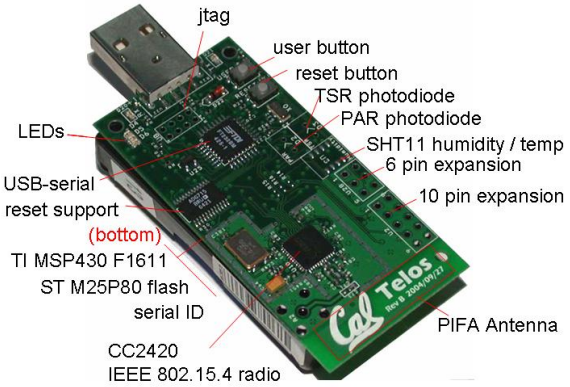

Figure 1.3.3: The TelosB sensor.

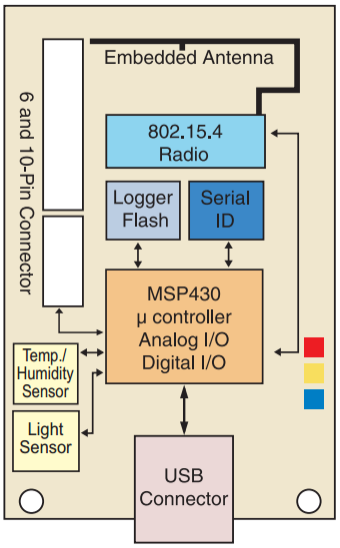

Figure 1.3.4: TelosB block diagram.

A gateway can be a PDA, a smartphone, a router, a computer, a server or any other machine that can play the role of connector of sensors or actuators devices, which are forming a local network between them, to access the Internet.

1.3.4 Medical Unit Center

End applications, following algorithms already established, will analyze the collected remotely data to treat, analyze it and give it in real-time to the final user, i.e. a caregiver or a health professional, in simple and understandable form to help him making decision, or as an alarm to warn of the need to act quickly before the patient's illness become too advanced to intervene.

The application must also provide an interface for defining and configuring the overall system behavior. What kind of alarms are generated and through which network the messages will be delivered, who are the target users, etc. are examples of the application configuration. In such a system, most of the problems mentioned in other subsystems are also involved.

The figure 1.3.5 summarizes the operation of an e-healthcare surveillance system in the context of the Internet of Things, the relationship between the different systems and communications established between them to collect information about the monitored person.

The table 1.3.1 summarizes the main design considerations for e-healthcare systems and the most important studies on this field [28].

1.4 Sensors: features and constraints

1.4.1 Smart sensor

A sensor is defined as a device performing the task of transforming a physical measurement observed in a generally electrical measurement that will in turn translated into a usable and understandable data for an information system and finally for a man.

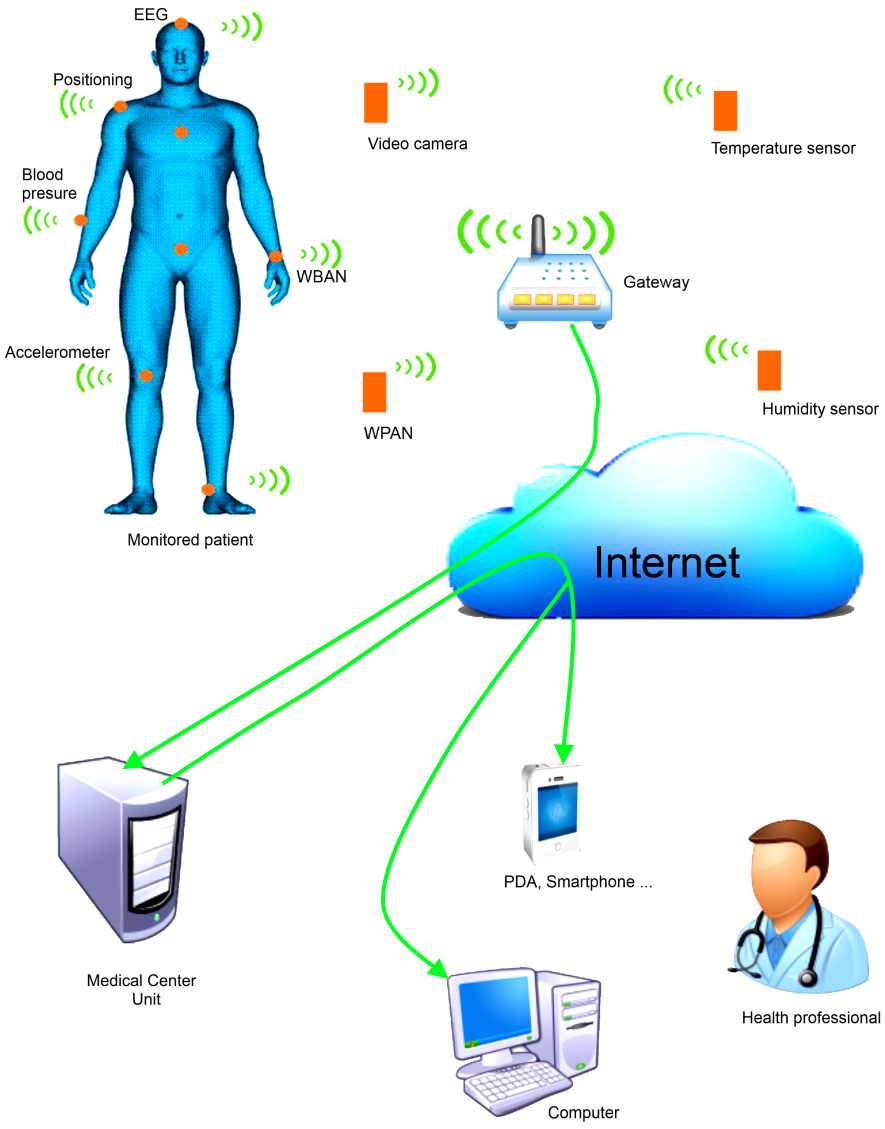

Figure 1.3.5: The e-healthcare systems in the Internet of Things context.

Subsystem	Design consideration
WBAN	Real-time availability Transmission power Power consumption Portability Unobtrusiveness Reliable communications Multi-hop routing Security.
WPAN	Energy efficiency Scalability Real-time availability Self-organization Security
Gateway	Congestion prevention Data rate Reliable communication protocols Secure data transmission Coverage Security
Medical Center Unit	Reliability User-friendliness Middleware design Scalability Interoperability Context-awareness Privacy Security

Table 1.3.1: The design considerations of an e-healthcare system.

In his work on industrial instrumentation, electronics Georges Asch [40], modeled precisely the notion of measuring instrument, and therefore that of the sensor (fig. 1.4.1). The physical quantity being measured, called the measurand m, is viewed by various experimental stages, grouped under the term of measurement, which in many cases produces an electrical signal s image of the physical quantity and its variations. The sensor that is the physical device subjected to the action of the measurand, nonelectric, product the electrical characteristic: s = F(m). Nevertheless, all physical laws interact in materials, so the sensor is necessarily sensitive to other secondary physical quantities, named influencing variables. The characteristic becomes, taking into account the influence of variables g_1, g_2, ...: s = F(m, g_1, g_2, ...). The main influencing variables are temperature, acceleration, vibration, humidity, magnetic fields.

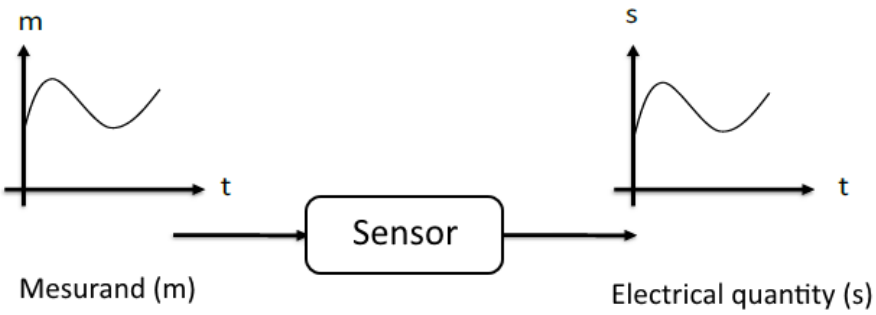

Figure 1.4.1: The functioning of a sensor.

Therefore, a sensor is a device equipped with advanced features sensation. It measures or detects a real event, such as motion, heat or light and converts the measurement into an analog or digital representation value. It collects information and develops from a physical quantity (input information), another physical quantity of electrical nature.

A smart sensor is a hardware device in which coexist a sensor and the circuits of processing and communication. Smart sensors are "sensors of information" and not just sensors processing circuits of juxtaposed signal [41]. In addition, their

components was designed with the goal of a very specific application.

1.4.2 Physical architecture

A smart sensor is composed of four units (fig. 1.4.2):

- *Acquisition unit*: consisting of a sensor that gets measures of environmental parameters and an Analog / Digital converter that converts the information recorded and transmits it to the processing unit.
- *Processing unit*: made up of a processor and a memory including a specific operating system (TinyOS [42], for example). This unit has two interfaces, an interface for the acquisition unit and an interface to the communication unit. It acquires information from the acquisition unit and sends them to the communication unit. This unit is also responsible for executing the communications protocols that allow the sensor to collaborate with other sensors. It can also analyze the captured data.
- *Communication unit*: a unit responsible for all transmission and reception of data over a radio communication medium. It can be optical (as in Smart Dust sensors), or radio frequency deviation (TelosB, for example).
- *Battery*: a sensor has a battery to power all of its components. However, because of its small size, the battery is limited and usually irreplaceable. For this, energy is the most valuable resource since it directly affects the sensors lifetime, so the network lifetime.

There are sensors that are provided with other additional components such as the positioning system GPS (Global Positioning System) and a mobilizer allowing it to move.

1.4.3 Main characteristics

Two entities are fundamental to the operation of a sensor: the acquisition unit, which is the physical heart to the measurement and communication unit, which

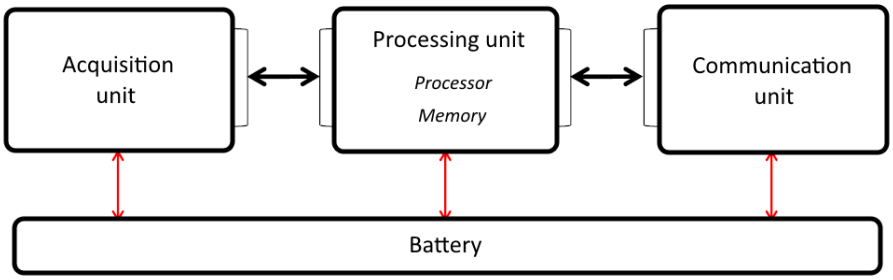

Figure 1.4.2: The physical architecture of a smart sensor.

performs the transmission thereof to other electronic devices. Thus, each sensor has a functionally communication radius (Rc) and a sensation of radius (Rs). Figure 1.4.3 shows the areas defined by these two radii for the sensor A. The communication area is the area where the sensor A can communicate with other sensors (sensor B). On the other hand, the sensing area is the area where the sensor can capture the event A.

Indeed, for a sensor having a sufficiently large range of communication, it is necessary to use a sufficiently powerful signal. However, the energy consumption is high.

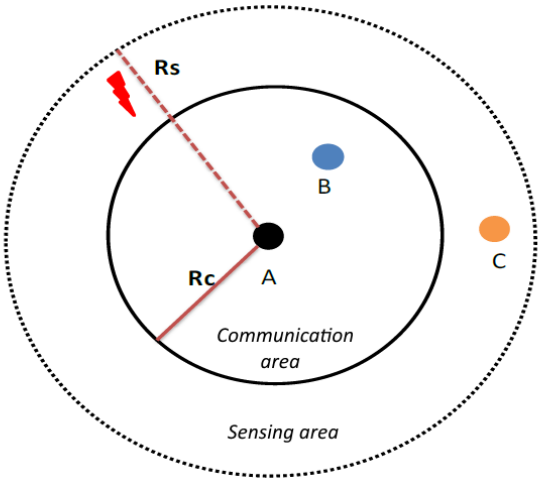

Figure 1.4.3: The wireless sensor communication and sensing areas.

1.4.4 LoWPAN: Low-power Wireless Personal Area Network

The LoWPAN (or LR-WPAN: Low-Rate Wireless Personal Area Network) are a special kind of ad-hoc network in which nodes generally are "smart sensors". They usually consist of a large number of sensors, depending the application, communicating with each other via radio links for information sharing and cooperative processing. In this type of network, sensors exchange information e.g. on the environment to build a global view of the monitored region, which is made available to external users with one or more nodes. Data collected by these sensors are fed directly, or through other sensors, to the "pickup point", called the base station (or sink case of a node). The latter can be connected to a powerful computer via Internet or satellite. In addition, users can send their requests to the sensors by specifying the information of interest.

Typically, the sensors are deployed in a random manner in an area of interest, and a base station, located at the end of this area, is charged to recover the data collected by the sensors. When a sensor detects a relevant event, an alert message is sent to the base station through a communication between the sensors. The collected data is processed and analyzed by powerful machines. Sensor networks are in support of the environment and the industry thanks to recent developments in the field of wireless technology. In recent decades, the need to monitor and control physical phenomena such as temperature, pressure or brightness is essential for many industrial and scientific applications.

1.4.5 LoWPAN networks characteristics

A sensors network has the following characteristics [43]-[45]:

- *Lack of infrastructure*: ad-hoc networks in general, and in particular sensor networks differ from other networks owned by existing infrastructure and lack of any kind of centralized administration.

- *Interference*: radio links are not isolated, two simultaneous transmissions on the same frequency, or in similar frequencies can interfere.

- *Dynamic topology*: the sensors can be attached to mobile objects moving in a free and arbitrarily thus making the network topology change frequently.
- *Limited physical security*: networks of wireless sensors are most affected by the security setting than conventional wired networks. This is driven by the constraints and physical limitations that make control of data transferred should be minimized.
- *Limited bandwidth*: one of the basic characteristics based on wireless communication networks is the use of a shared communication medium. This sharing makes the bandwidth reserved for a node very limited.
- *Energy, storage and computation constraints*: the most critical feature in sensor networks is the modesty of its energy resources since each sensor network has low resources in terms of energy (battery). To prolong the life of the system, a minimization of energy expenditure is required in each node. Thus, the storage capacity and computing power is limited in a sensor.

1.5 Summary

In this first chapter, we put light on the concept of the Internet of Things and its application in the field of e-healthcare. We also have introduced sensors devices that was the subject of our work by addressing their operations and constraints. The first objective by creating the Internet of Things and the development of its mechanisms is to make sensors more autonomous and independent devices from the human user direct control, and enable him to monitor and remotely control these devices. The other advantage of this trend is that it will offer the maximum information and hence help in decision making. The highlight of the Internet of Things is its impact on many aspects of everyday life.

Like anything new, the Internet of Things recognizes several problems; the main one being how to ensure full interoperability of devices interconnected while respecting their adaptive character and autonomous behavior in a secure and confidential environment. In addition of issues related to its implementation. "Things"

that make up the Internet of Things are characterized by low energy resources. Therefore, the solutions proposed must pay attention to this critical character.

A technology called "6LoWPAN" (IPv6 over Low-Power Wireless Personal Area Network) was created and developed by the Internet Engineering Task Force (IETF) to allow these devices to obtain a personal IP address and connect to the Internet. The intervention of the Internet of Things will be a revolution in many fields such as industrial and structural monitoring, environmental monitoring, automotive telematics, automation, etc., but its contribution is of great promise in the e-healthcare domain, where its principles are already applied to facilitate access to care, improve its quality and reduce its cost.

E-healthcare applications are aimed to reform existing healthcare services by offering remote monitoring for patients at risk to target diagnostic and therapeutic. The automation of data collection will reduce the risk of human error that can sometimes be fatal in the healthcare field.

Many devices and systems must work together in the context of the Internet of Things, to contribute to the improvement of the entire healthcare system. Application monitoring of end-user health needs a diverse set of information on individual supervised conditions and environment in which he is located, to get an idea of his condition and the type of intervention should be taken. Information will be collected by a range of different types of sensors, each according to its application. Most existing solutions include one or more types of sensors worn by the patient composing the Body Area Network (BAN), and a group of types of sensors deployed in its environment forming a Personal Area Network (PAN). These two elements are connected to a core network via a gateway, which connect to the Internet. In addition, a Medical Center Unit (MCU) that receives the detected information, process it, analyze it and stored it in a database. At the application level, health professionals or other caregivers can monitor vital health information in real time from the patient via a Graphical User Interface (GUI).

Unfortunately, the characteristics of sensor networks poses many challenges such as lack of infrastructure and the lack of any form of centralized management, the sensors can be attached to mobile objects moving in a free and arbitrarily thus

making the network topology changes frequently, limited physical security devices minimized and deployed in insecure environments,etc. The most critical feature in sensor networks is the modesty of its energy resources. To prolong the life of the system, a minimization of the energy expenditure is required in each node.

In the next chapter, we will give an overview of 6LoWPAN technology that offer the Internet connection ability to the wireless sensors, its objectives and mechanisms, various problems and how they are been treated. We will give answers to the following question: what is the 6LoWPAN and why it was been developed ?

We're still in the first minutes of the first day of the Internet revolution.

Scott D. Cook

2

6LoWPAN overview

Future sensor networks, with thousands of nodes will be connected to others via the Internet of Things. Therefore, an efficient addressing mechanism is needed to communicate with the other IP-based sensor nodes. Consequently, the IETF IPv6 over Low power WPAN (6LoWPAN) working group was convened to define the transmission of IPv6 packets over IEEE 802.15.4 resource constrained networks. However, the combination of the two IPv6 and IEEE 802.15.4 networks wasn't an easy task, many challenges obstruct this idea as the two networks are totally different, the IPv6 protocol was designed for powerful devices, on the other side, IEEE 802.15.4 standard was designed especially for resource constrained devices.

2.1 Introduction to 6LoWPAN

In order to make the concept of the Internet of Things a reality, several projects operate in parallel, most notably the integration of devices with limited resources to Internet. Obtaining information from any environment (sensing) and acting on anything physical (actuating) will be possible. For this, the Internet Engineering Task Force (IETF) establishes a working group under the name of 6LoWPAN, i.e. IPv6 over Low-power Wireless Personal Area Networks [23] (fig. 2.1.1 [46]).

2.1.1 The choice of the IPv6

The choice of IPv6 protocol [47] was the result of several considerations and advantages summed up in the fact that devices equipped with IP can link directly to the Internet without the need to an intermediate or a gateway. In addition, the Internet and everything about it has been developed for years and has spread across the world, several people are working on it as researchers, technicians, organizations and companies to improve its quality, the integration of these devices to the Internet will take advantage of these available infrastructure.

Among the most important advantages, the IP is a free open source protocol and does not possessed by any specific organization. All documents relating to its properties operations are available to the public, every person has the opportunity to use it or develop it, which creates a competition and encourages innovation and development.

Regarding the adoption of IPv6, it is a strategic choice rather than technical, the IPv4 consists of 32 bits, it allows 2^{32} addresses, i.e. approximately 4.3 billion addresses. But, with the proliferation of the Internet for a large scale, the huge increase in the number of its users, and the emergence of a large number of devices that can connect to the Internet such as smartphones, tablet computers and videogames consoles is accompanied by a depletion of IPv4 addresses, i.e. the gradual saturation of the amount of available public IPv4 addresses. Saturation threatens the growth of the Internet. In February 2011, the reserve of free blocks

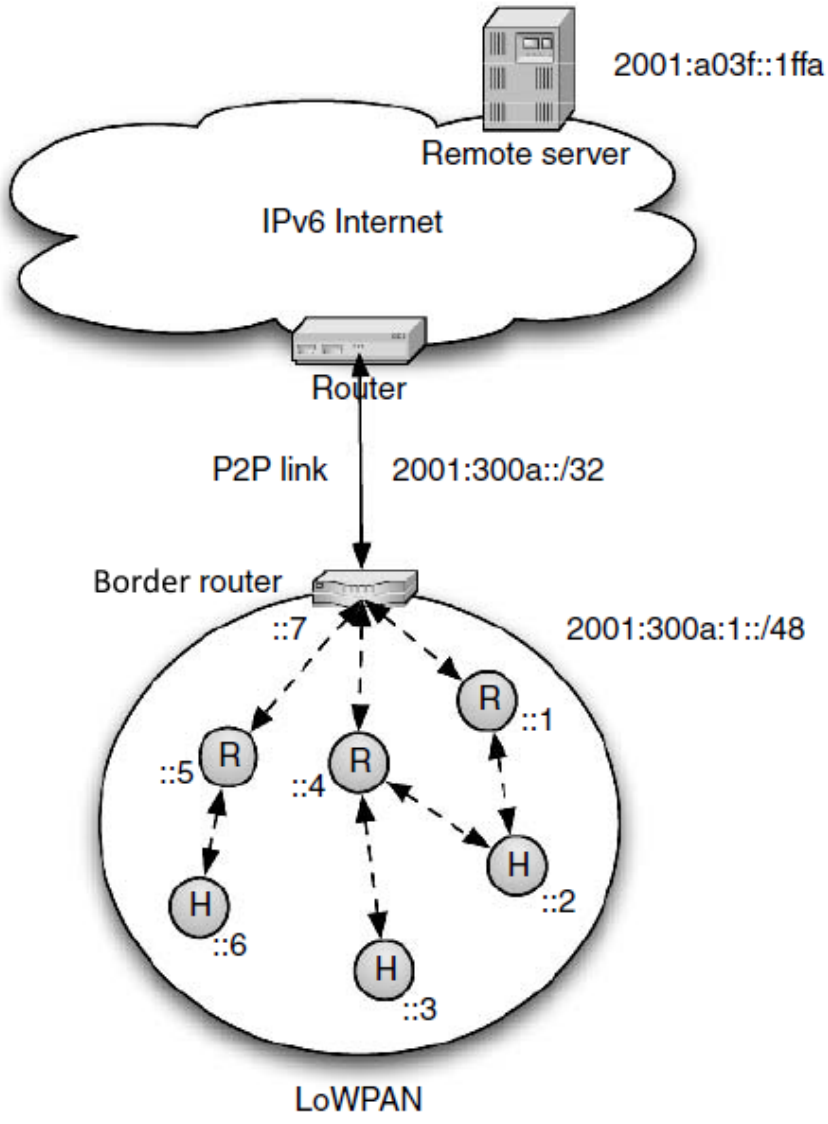

Figure 2.1.1: A 6LoWPAN network example.

of IPv4 public addresses from the Internet Assigned Numbers Authority (IANA) [48] has reached exhaustion [49]. The number of devices able to connect to the Internet within the Internet of Things will double to a million times what it is currently the case. It was needed to upgrade to IPv6 version composed of 128 bits, which will allow access to nearly 2^{128} addresses, about 3.4 10^{38} addresses. This equates to an unlimited number as to saturate the system, to reach the limit, it should be placed over 667 million of billions Internet-connected devices over every square millimeter of earth surface.

2.1.2 Integration challenges

However, in spite of all these advantages, the integration of IP within devices with limited resources is not an easy thing because of the many challenges faced by the 6LoWPAN working group. The Internet available protocols are designed for devices with high capacity and did not take into account the devices with limited resources. The first challenge formed in the large size of the IPv6 packet capacity compared to devices based on IEEE 802.15.4 standard in determining their data link layer that its frame capacity is 127 bytes in maximum. Most of wireless resource-constrained devices are based on the 802.15.4 standard that was designed specifically for this kind of devices. In addition to many other requirements imposed by the nature of the 802.15.4-based devices and all the resources-constrained devices. These requirements are not considered as deficiency, but the nature of their operation imposed these characteristics. Most of these devices are a collection of wireless small-scale low-cost machines able to collect and send sensed data in its environment, able to withstand a very long time without any human intervention due to its low energy batteries, and thanks to its programmed system that was designed to let them interact with their environment and the surrounding devices automatically.

These characteristics put obstacles in front of their integration into the Internet, its low capacities and its low power consumption makes it difficult to apply the standard Internet protocols, it relies on algorithms with complicated compu-

tations and therefore excessive use of the processor and the memory. In addition, the impossibility of being linked to the Internet all the time as they go in sleep cycles to maintain their batteries for the longest time possible. Some devices are used only once as they are put in places difficult to access, and thus the impossibility of changing the batteries. Sometimes, the price of access to the device and charge its battery is more expensive than the device itself.

Another problem is formed in the bandwidth where devices with limited resources, has a limited range (20 - 250 Kbytes/s), which limits the amount of data can be sent in a one frame. Finally, one of the challenges that are related to the characteristics of devices with limited resources is the reliability in the sending and receipt of data. The weak characteristics nature of wireless communication, the lack of reliable infrastructure, the weak capacity of the devices, and its frequent and long sleep cycles makes reliability factor an important and a major challenge.

2.1.3 Solution and requirements

Despite all these challenges, IPv6 still the perfect choice for devices with limited resources to connect to Internet. The following paragraphs will explain how IETF 6LoWPAN WG handles with these challenges through 6LoWPAN technology, which through it and by the adaptation of the rest of the protocols relating to IPv6 or by finding new ones, it became possible for resource-constrained devices and limited resources networks connect to the Internet. The premises and the goals that the 6LoWPAN WG was envisaged and the challenges and problems posed in order to normalize 6LoWPAN are accessible through RFC 4919 [50] and RFC 4944 [51] documents. These documents lists goals and initial problems. The team collaborates with many researchers, academics, companies and institutions in order to solve these issues.

6LoWPAN is a set of standards that allow the use of IPv6 in devices with limited resources, hence its name "IPv6 over Low-power Wireless Personal Area Networks". In 2007, the first 6LoWPAN specification was issued in two versions; the first was in RFC 4919 document, which contains the requirements and objectives

of the networks with limited energy to connect the Internet, and hypotheses developed to achieve these goals. Moreover, the problems and challenges as connectivity, topology, the limited size of the packets, the limited management mechanisms, network configuration and security problems.

Followed by another document RFC 4944 that describes the format of transmission frame of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly autoconfigured addresses on IEEE 802.15.4 networks. In addition of other specifications include a simple header compression scheme using shared context and provisions for packet delivery in IEEE 802.15.4 meshes. This document has been updated through two other documents illustrate more these additions, RFC 6282 [52] document in 2011, which specifies an IPv6 header compression format for IPv6 packet delivery in Low Power Wireless Personal Area Networks (6LoWPANs). This document specifies compression of multicast addresses and a framework for compressing next headers. UDP header compression is specified within this framework. The other document RFC 6775 [53] in 2012 describes simple optimizations to IPv6 Neighbor Discovery protocol [54], its addressing mechanisms, and duplicate address detection for Low-power Wireless Personal Area Networks and similar networks.

Among the major challenges faced by the IETF is the routing. The IETF established a new working group under the name of ROLL (Routing Over Low power and Lossy networks) in 2008 to search for a new protocol agrees resources-constrained networks requirements while taking into account the characteristics of 6LoWPAN. The ROLL working group reached the first scheduled version of the protocol in 2012 called RPL (IPv6 Routing Protocol for Low power and Lossy Networks) described in RFC 6550 [54]. This protocol provides a mechanism whereby multipoint-to-point traffic from devices inside the Low power and Lossy Networks (LLN) towards a central control point, as well as point-to-multipoint traffic from the central control point to the devices inside the LLN, is supported. Support for point-to-point traffic is also available.

2.1.4 Security issue

During this time, IETF 6LoWPAN WG reaches definitive solutions for most of these requirements. However, the problem of security is still an open field because the difficulty of applying one specific solution on all applications. The last draft document about security was in 2011 [55], which discusses possible threats and security options for IPv6-over-IEEE 802.15.4 networks. Other security drafts documents concern analysis of the security issues regarding RPL routing protocol, the latest version was in the current year (2014) [56].

The beginning of interest as evidenced by the shown documents was for IEEE 802.15.4 networks, used specially in what is known as "Wireless Sensor Networks" (WSN) [57] that knew a huge evolution and a major development since the 1990's. It has become an important field of scientific research referred to in all areas. However, research in the field of LoWPAN networks, especially the cited WSN, was always been studied as an independent network that operate in isolation from the rest. Its goal is sensing the target environment, and send data to the base station where they are collected and sent for analysis.

The field of LoWPAN remained a scientific academic research field until those companies began to bother it and became interested in the commercial field. Especially those sensor devices are low cost machines in terms of processing, as well as in terms of functioning, and provide very important monitoring services. Thus, LoWPAN networks emerged from research areas concerning only researchers in their respective fields, to the outside world where merged industry fields, environment, healthcare, and even entertainment. As the trend in the world is facilitating the means of communication and make them accessible to everyone, it was inevitable that LoWPANs has been oriented to be integrated to Internet.

The goal become how to access to the device itself, which will allow access to more accurate data in real-time, instead of getting information through the base station. The other goal is what we talked about earlier about landing the concept of "Internet of Things" to the reality, where each device will be able to communicate directly with any other device in end-to-end manner without any intermediary,

which will provide more autonomy and faster communication. For this purpose, i.e. the integration of 802.15.4 networks into the Internet, the IETF created 6LoWPAN WG to deal with this project, involving major corporations, universities and scientific research centers.

2.1.5 6lo: 6LoWPAN successor

Despite the fact that 6loWPAN has developed in order to deal with devices based on 802.15.4, in the beginning of the current year (2014), it was began to prepare its generalization to all resource-constrained devices through the 6lo project (IPv6 over Networks of Resource-constrained Nodes) [58]. 6lo is also an IETF working group that collaborate many teams in order to mainstream 6LoWPAN solution to all devices with limited resources in order to enable them to connect to the Internet. These teams are working on these projects:

- Transmission of IPv6 over MS/TP Networks [59].
- Transmission of IPv6 Packets over BLUETOOTH(R) Low Energy [60].
- Transmission of IPv6 Packets over DECT Ultra Low Energy [61].
- 6LoWPAN Generic Compression of Headers and Header-like Payloads [62].
- Definition of Managed Objects for 6LoWPANs [63].
- Transmission of IPv6 packets over ITU-T G.9959 Networks [64].
- Transmission of IPv6 Packets over Near Field Communication [65].
- 6LoPLC: Transmission of IPv6 Packets over IEEE 1901.2 Narrowband Powerline Communication Networks [66].
- IPv6 mapping to non-IP protocols [67].

2.2 6LoWPAN architecture

The 6LoWPAN networks are created by connecting islands of wireless sensor devices, each island is presented on the Internet as a stub network, which is a network that IP packets are sent to or from its destination, but which does not act as a way to other networks. The 6LoWPAN architecture is made up of LoWPAN network(s) (fig. 2.2.1).

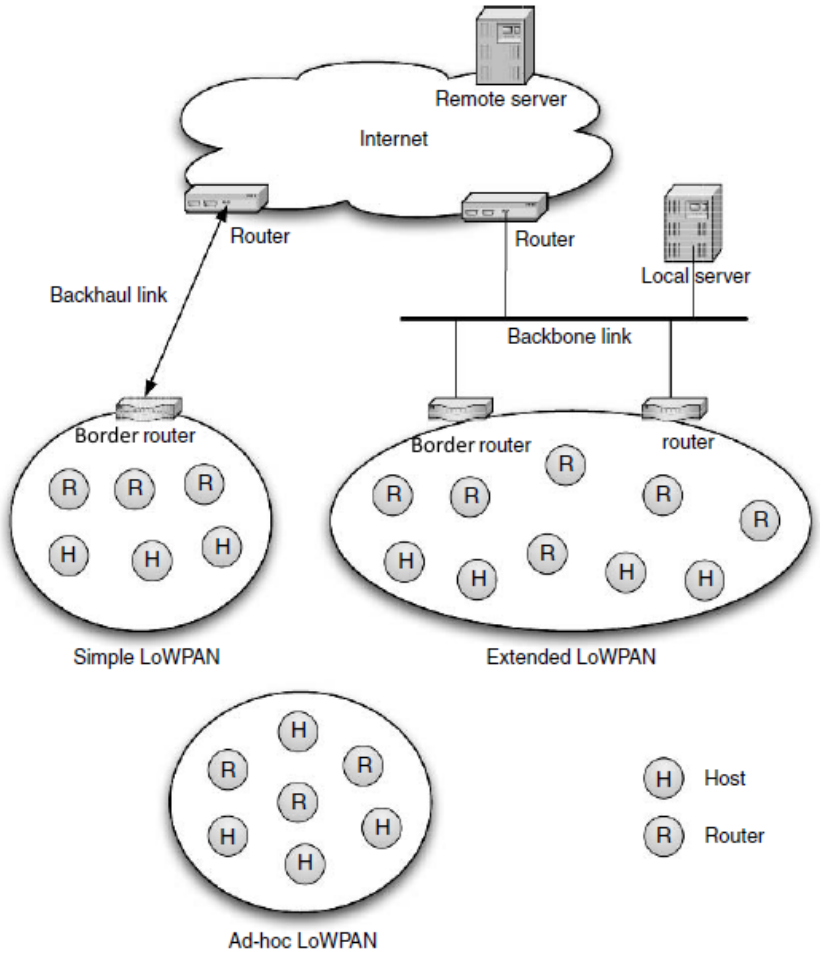

Figure 2.2.1: The 6LoWPAN architecture.

2.2.1 Network components

In order to get on the 6LoWPAN network, we must have a LoWPAN network that combines two types of resource-constrained nodes: host and router. The host device, which is the end point of the network, its function is to gather information or carry out the orders, it does not act as a link with other devices. Instead of the other type, a router, which acts as a link between the devices and is essential in high-density networks. During the distribution, it must that any host device to be associated with at least a router; otherwise, it will be outside the reach of the network. This division of the devices came agree to the division of that it is in 802.15.4 standard, which divides devices into two types: a FFD (Full Function Device) that can play the role of the sensor and the role of the router, and RFD (Reduced Function Device) that can play simple roles as sensing only, it is considered as an end device.

2.2.2 Communication mode

These nodes communicate with each other through a wireless communication organizing in ad hoc, i.e. without having any infrastructure. They share the same IPv6 prefix. Regarding communication with other IP networks, it is established through the 6LoWPAN Border Router (6LBR). It was called "border" because it forms the boundary between the internal network; the LoWPAN, and the external network; the Internet. The 6LBR is a powerful machine, responsible for determining the IPv6 prefix and its distribution to the nodes, assumes the role of the monitor and the controller of the LoWPAN, regulates sent or received packets traffic, supports compression operations of the header of the packet, manages Neighbor Discovery protocol operations, where each node in the LoWPAN must apply to register in the 6LBR database, and manages the communications with IPv4 networks.

More than one 6LBR can exist in a LoWPAN, linked to a backbone that could be an Ethernet link, and share the same IPv6 prefix, and attached all to a router that linked them to the Internet. This router handles Neighbor Discovery node registration requests. It makes it easier for nodes movement within the LoWPAN,

without the need to re-register each time in the 6LBR and change the IPv6 address. It allows the construction of LoWPAN networks with several nodes and several 6LBR, which share the same IPv6 prefix. So the node can move into the LoWPAN without changing its IPv6 address.

Communication between LoWPAN nodes and the rest of the IP-based devices in other networks occur in end-to-end manner like any two IP-based devices. It is among the advantages of IP-based networks where the device must only obtain an IP address to communicate with any other device available without relying on a gateway or a middleware.

2.2.3 Network topology

6LoWPAN can operate without infrastructure, it can also function as an ad hoc LoWPAN. In this topology, a simplified 6LBR is used, which implemented two basic functions: the generation of a Unique Local Unicast address (ULA) [68] and handling 6LoWPAN Neighbor Discovery registration functionality.

The network topology may change due to several factors, among them the moving nodes, since nodes can register in several LoWPAN simultaneously, which called multi-homing. The nodes can move within the network between the 6LBRs, and even between LoWPANs. The topology may change also due to wireless channel conditions without that a node performs a physical movement. A multi-hop mesh topology in LoWPAN is achieved either by link-layer forwarding; called Mesh-Under, or by using the IP routing; called Route-Over.

2.3 6LoWPAN protocols stack

The 6LoWPAN protocol stack (fig. 2.3.1) is approximately the same in comparison with a typical IP protocol stack and the corresponding five layers of the Internet Model (the four-layer model of RFC 1122 [69] with a physical layer separated out of the link layer) with the addition of the new layer: the adaptation layer, called also the 6LoWPAN layer. Adaptation between full IPv6 and the 6LoWPAN format is performed by routers at the border of LoWPAN islands in the 6LBR routers

(fig. 2.3.2).

6LoWPAN stack layers consist of IEEE 802.15.4 PHY layer, IEEE 802.15.4 MAC layer, adaptation layer (6LoWPAN layer), network layer, transport layer and application layer.

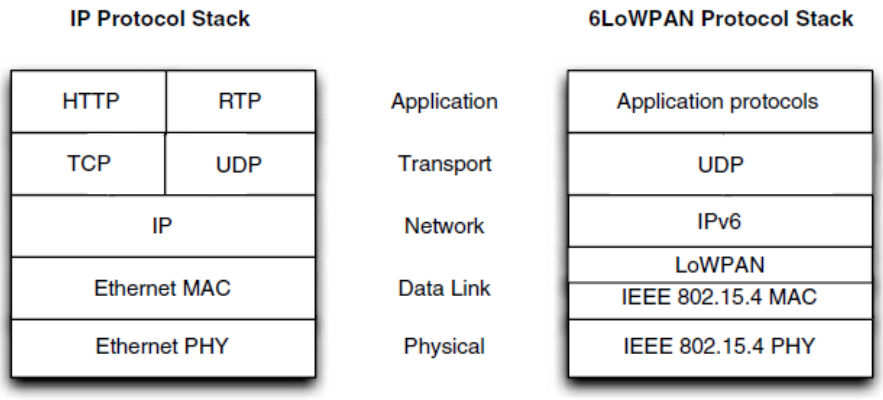

Figure 2.3.1: IP and 6LoWPAN protocols stack.

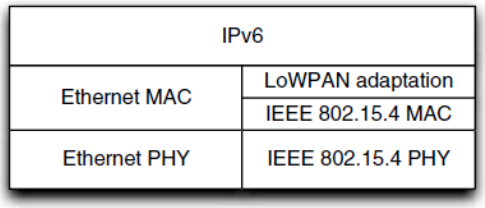

Figure 2.3.2: Border router with 6LoWPAN support.

2.3.1 Physical layer

The 6LoWPAN physical layer, it is commonly abbreviated PHY, provides two services: the physical data service and the physical management service interfacing to the PLME-SAP (Physical Layer Management Entity - Service Access Point). The physical data services provide the reception and transmission of data packets

between MAC and PHY through the physical radio channel. The physical management service interface provides access to all layer management functions; also, it maintains a database of personal area networks information. It is based on the IEEE 802.15.4 standard, with a data rate of 250 kbps.

The PHY manages the physical RF transceiver and performs channel selection, energy, and signal management functions. It operates on one of three possible unlicensed frequency bands:

- 868.0–868.6 MHz: Europe, allows one communication channel (2003, 2006, 2011)
- 902–928 MHz: North America, up to ten channels (2003), extended to thirty (2006)
- 2400–2483.5 MHz: worldwide use, up to sixteen channels (2003, 2006)

2.3.2 Data link layer

6LoWPAN data link layer, called also the MAC sublayer, provides two services: the MAC data service and the MAC management service interfacing to the MAC sub-layer management entity (MLME) service access point (SAP), the MLME-SAP. MAC data service provides the transmission and reception of the MAC protocol data units (MPDU) through the PHY service data. The IEEE 802.15.4 provides monitoring services transmissions by defining four frame structures for the MAC layer:

- *Data frames*: to transfer the actual data.
- *Acknowledgment frame*: sent from the data receiver, if requested by the sender, in the successful reception of the data frame.
- *Command frame*: used by most data link layer services in order of correlation or separation of a device from its coordinator.

- *Beacon frame*: used by coordinator to organize communications with the devices attached to it.

The MAC determines as well the physical address of the device, and supports two types of addresses, the EUI-64 [70] identification address consisting of 64 bits, and the short address of 16 bits. In addition to other services related to the management, security and addressing that will be addressed in the next paragraphs. The MAC also provides the Frame Check Sequence (FCS) service. The IPv6 information is allocated in the payload; the MAC service data unit (MSDU) (fig. 2.3.3, fig. 2.3.4 [71]).

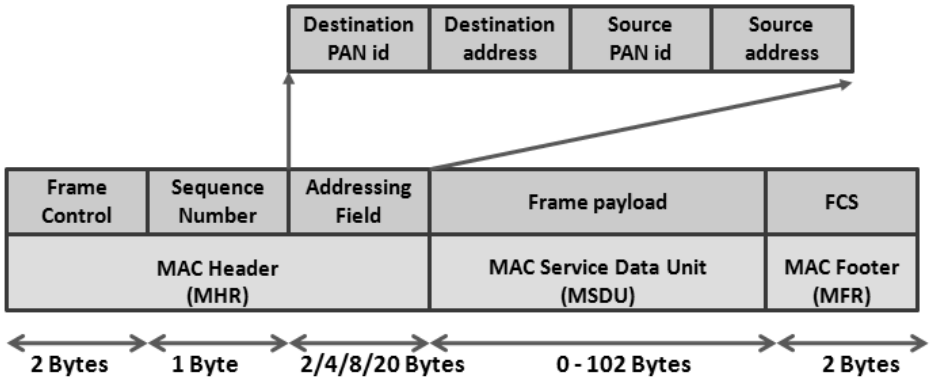

Figure 2.3.3: General MAC frame format.

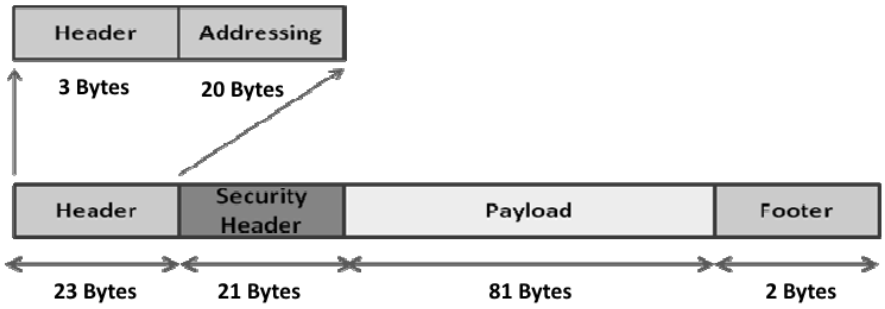

Figure 2.3.4: IEEE 802.15.4 frame format.

2.3.3 Adaptation layer (6LoWPAN layer)

The 6LoWPAN format delineate on IPv6 communication is carried in 802.15.4 frames and identifies the main elements of the adaptation layer. 6LoWPAN has these main elements:

2.3.3.1 Fragmentation and reassembly

IPv6 packet size is 1280 bytes. Therefore, the packet size is larger than the frame of the IEEE 802.15.4 standard. Under these conditions, the size of the IPv6 packet unable to be encapsulated in an IEEE 802.15.4 frame. 802.15.4 protocol data units have variety of sizes as It depends on the overhead occurred. Its Maximum Transmission Unit (MTU) is 127 bytes. This frame has 25 bytes, header, footer and addressing overheads. Moreover, if AES-CCM-128 [72] is used; security header imposed by data link layer adds 21 bytes overhead. Therefore, the rest for the payload is 81 octets.

With these mechanisms, for that the IPv6 to be transmitted on the IEEE 802.15.4 frame; it must be divided to more than 16 fragments. Therefore, the adaptation layer has to manage the process of fragmentation and reassembly. It was created in order to receive the IPv6 packets, fragments them in the transmission, and reassembles them at the reception.

2.3.3.2 Header Compression

IPv6 packets must be performed on the data frames. After that the packet is been fragmented, it is transmitted over IEEE 802.15.4 frames where each fragment carries a part of the original IPv6 packet. The IEEE 802.15.4 frame has a maximum packet size of 128 bytes; instead IPv6 header size is 40 bytes, User Datagram Protocol (UDP) [73] and Internet Control Message Protocol (ICMP) [74] header sizes are two of 4 bytes, fragmentation header add another 5 bytes overhead. Without compression, 802.15.4 is not able to transmit any payload effectively.

2.3.4 Network layer

6LoWPAN network layer provides the ability to interconnect networks of sensor nodes. Its main activities are addressing and routing..

The IP packet is fragmented, the fragments are sent to the next hop based on routing table information. If the adaptation layer in the next hop successfully received all the fragments, it creates an IP packet from these fragments and sends it to the network layer. Thereafter, the network layer sends the packet to the upper layer, the transport layer, in the case of the packet is destined for it. In the other case, it forwards the packet to the next hop. If there are missing fragments, all fragments are forwarded to one hop distance.

2.3.5 Transport layer

The transport layer is responsible for the delivery process to process. It outputs a data segment to the destination node to the suitable application process. There are two protocols that occurs in this layer; User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) [75]. In the source side, the use of TCP or UDP protocol depends on the application.

The data of the application layer are organized in the UDP or TCP segments. On the destination side, the transport layer receives the segments from the network layer. It processes them depending on the used protocol and sends the result to the proper application layer.

In the aspect of complexity, efficiency and performance, UDP is the most used protocol in 6LoWPAN networks as TCP is not preferable to be used in resource-constrained networks.

2.3.6 Application layer

The 6LoWPAN application layer uses a socket for each application in order to send and receive packets. The socket is associate with the used transport layer protocol (UDR or TCP) and source and destination ports.

Application protocols are equally important for 6LoWPAN. However, limitations such as limited memory, limited data rates, small frame sizes, and sleeping node cycles make the development of new application protocols and the adaptation of existing ones very difficult (fig. 2.3.5). Furthermore, the autonomous nature of these devices makes autoconfiguration, manageability and security all-important. Although, most of standard applications protocols was adapted and are becoming available, like HyperText Transfer Protocol (HTTP) [76], File Transfer Protocol (FTP) [77], Session Initiation Protocol (SIP) [78], Real-Time Protocol (RTP) [79], Service Location Protocol (SLP) [80] and the Simple Network Management Protocol (SNMP) [81].

2.4 Addressing

Since 6LoWPAN devices depend on both IPv6 protocol and IEEE 802.15.4 standard, it supports the address provided by each of them. It supports the 128 bytes IPv6 address; it defines the node address in the network when it is connected, and it is responsible for transfer packets from end to end, the 64 bytes EUI-64 identification address; it defines the node, and the 16 bytes short address prepared for the inter correspondence; it is considered optional, and it is used only in the case of its configuration was requested.

2.4.1 Address composition

For the EUI-64, the manufacturer assigns it to each device, and it must be unique. The manufacturer must buy the OUI (Organizationally Unique Identifier) serial number [82], consisting of 24 bits, it is added to another 40 bits number chosen by the manufacturer himself. The IPv6 can be configured through a combination of EUI-64 and the 64 bits IPv6 prefix (fig. 2.4.1). The IPv6 prefix specify the address of the network to be distinguished from other IP networks, Its configuration depend on many methods described in RFC 3633 [83], RFC 6603 [84] and RFC 3769 [85]. The 6LBR is responsible for identifying this prefix to its nodes.

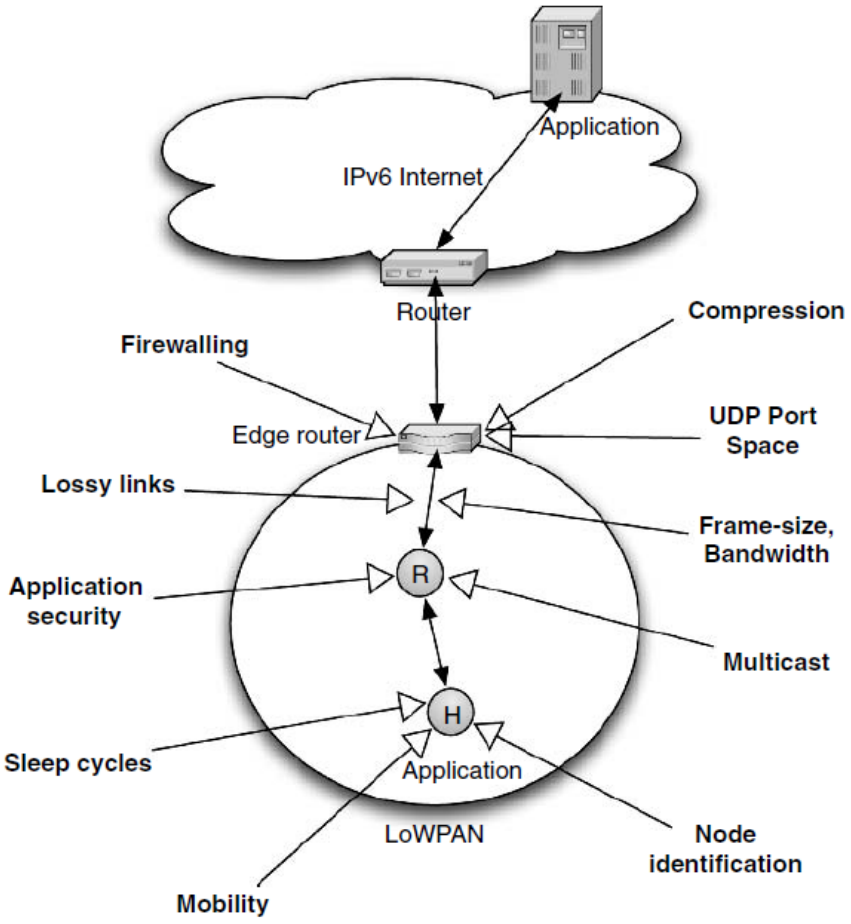

Figure 2.3.5: Application design issues to consider and where they occur in a LoWPAN.

2.4.2 Address configuration

In order to avoid any errors in the installation of addresses and make sure of its uniqueness, the 6LBR relies on mechanisms of IPv6 Stateless Address Autoconfiguration [86], it specifies the steps a host takes in deciding how to autoconfigure its interfaces in IPv6. The autoconfiguration process includes generating a link-local address, generating global addresses via Stateless Address Autoconfiguration, and the Duplicate Address Detection (DAD) procedure to verify the uniqueness of the addresses on a link. Note that this way of the formation of the IPv6 addresses is a convention but is not mandatory. The Neighbor Discovery protocol is used for exchanges between nodes and the 6LBR in order to ensure the uniqueness of the address.

```
2001:0DB8:0BAD:FADE::                    -- Prefix (/64)
                     ACDE:4812:3456:7890 -- EUI-64
2001:0DB8:0BAD:FADE:ACDE:4812:3456:7890 -- IPv6 Address
```

Figure 2.4.1: Composition of an IPv6 address from a EUI-64.

2.5 Autoconfiguration

A 6LoWPAN node that was implemented in a network should (not necessarily in this order):

- find the LoWPAN it will be part of;
- establish parameters such as the IP address prefix and its own IPv6 address;
- establish security associations with the relevant entities in the network;
- build paths on the node to relevant entities, to maintain existing roads and perhaps begin to transmit to other nodes in the network;
- establish the parameters of the application layer;

- establish security associations with other entities at the application layer;
- start the application layer protocols.

Part of this state implementation must be repeated dynamically in small time scales, such as the selection of the router and the routing paths.

The routing path selection is performed using a routing protocol, which can also assist in the selection of the router. Other parameters are less dynamic. Their setup can be structured into two phases:

- *Commissioning:* part of the state establishment that will require human intervention. This is also the time when security relations are initialized, which will protect the network and devices and applications against the attackers and accidents.
- *Bootstrapping:* after commissioning, the node is configured to operate without human intervention. However, it may still be state that must be acquired, either when initializing the device (power-up with new batteries) or when it joins a LoWPAN.

Note that there are a range of activities required to make a node in service, and it is not always clear whether a particular activity is commissioning, bootstrapping, or a part of a dynamic protocol such as routing. However, there is an IPv6 protocol that is clearly linked to the bootstrapping: Neighbor Discovery. This protocol has been optimized for 6LoWPAN. Both the commission and the boot has a strong relationship with security.

2.5.1 Commissioning

Most 6LoWPAN devices will be manufactured as generic devices, so they will leave the factory without any information that would enable them to function in a specific context. The process to provide this information may be part of what is called configuration. A LoWPAN device must have some way to identify the network

and information security. Often, it will not search for channels for available networks, but be statically configured to a specific channel. There is no such thing as a Service Set Identifier in IEEE 802.15.4; instead, a node can assume that it found its network when security settings and keying materials match. In addition to allowing the unit to attach to the desired LoWPAN, it may need to adjust its settings for applications to find the appropriate peers. One way to perform the commissioning is to set up devices during production, it can be a very efficient process. The downside is that any disruption of this process, as a defective or damage during installation requires an exceptional process or maybe even wait for the new production.

An alternative is to deliver units in a non-configured state and make setting specific service target during delivery, or during installation at the target. Finally, the device could be implemented using the in-band communication, i.e., using the 6LoWPAN communication. It is difficult to put into service in this way both automatic and secure, like a completely generic device cannot be distinguished from another device completely generic.

2.5.2 Bootstrapping

The IPv6 Neighbor Discovery protocol [54] is a focal point in the bootstrapping of an IPv6 network. A node uses Neighbor Discovery (ND) to discover other nodes on the same link, to determine their link-layer addresses, to find routers and to maintain reachability information about access to neighboring paths that node actively use to communicate.

The basic ND protocol divides nodes into hosts and routers, where only the router forwards the IP packets that are not addressed to itself. Routers must perform some additional features compared to ND hosts. As many nodes in LoWPANs will be limited in their abilities, 6LoWPAN-ND [53] introduces a third role, that of border router, which is specialized to perform some of the most complex 6LoWPAN-ND functions, reducing the complexity of the tasks be done by the other routers and hosts in particular. The new main concept is that of the white-

board held by the border router to centralize some of the protocol state.

2.5.2.1 Registration

In the standard ND, routers periodically send Router Announcements (RA), and if they do not want to wait for the periodic RAs, nodes can seek a router by Router Solicitation (RS) message. Both messages are usually multicast. In this case, this does not pose a problem, even in LoWPANs: communication occurs between the host and the first-hop router, so no expensive multi-hop message transfer is required. The next step after the formation of an address would be to perform Duplicate Address Detection (DAD) mechanisms. This is done by sending a Neighbor Solicitation (NS) to a solicited-node address, a multicast address formed based on the address to confirm. This process works correctly if multicast packets are likely to reach all nodes subscribing to the solicited-node address on the subnet, an assumption that cannot be done for 6LoWPAN. Instead, the 6LoWPAN-ND uses border routers as the focal point of the DAD. Each border router maintains a whiteboard on which nodes can scribble their address and other nodes can read later. This is done using two new ICMPv6 [87] messages: Node Registration (NR) and Node Confirmation (NC); the whole process is accordingly called registration (fig. 2.5.1).

2.5.2.2 Multihop registration

The registration process is a bit more complicated when registering node is not adjacent to the border router. Nodes can register to a LoWPAN router in the one-hop neighborhood as a router indicates its ability to manage the registration. The router then forwards the NR for the border router and the NC to the node. When a node sends its first message NR, its link-local address is always optimistic. Therefore, the node sends the NR with the source IPv6 address set to the unspecified address. The relaying router takes note of the NR and the source link-layer address that should directly map into each other, and uses this state to relay the NC re-

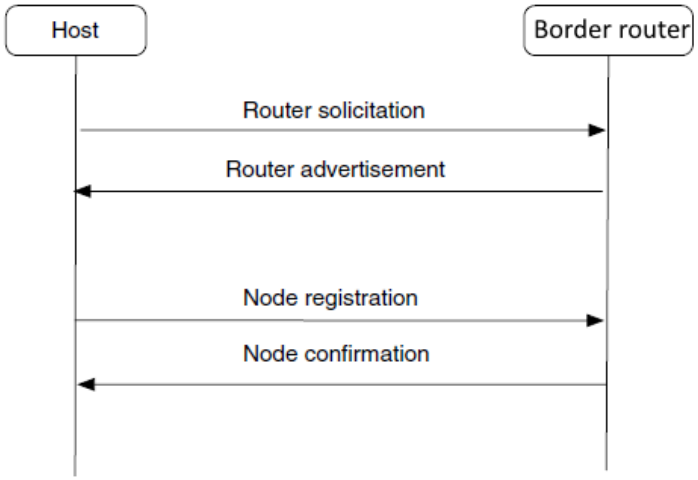

Figure 2.5.1: Basic router discovery and registration process with a border router.

sponse later from the border router to the correct link-layer address for the node (fig. 2.5.2).

2.6 Devices operations

2.6.1 Node operation

LoWPAN nodes start by autoconfiguring the link-local address derived from the globally unique EUI-64 of the LoWPAN interface. From the point of view of Stateless Address Autoconfiguration, link-local address begins as an optimistic address [88] and requires confirmation by an exchange of NR / NC messages with the border router before becoming operational. Assuming that the global prefix for LoWPAN is known at this stage, the same exchange NR / NC can also be used to record the address prefix of the overall compound and the same modified EUI-64. Finally, the node can go ahead and request the assignment of a link-layer 16-bit short address of the border router by recording an address consisting of the global prefix and the ID consists of PAN ID (usually zero) and 16-bit short address to

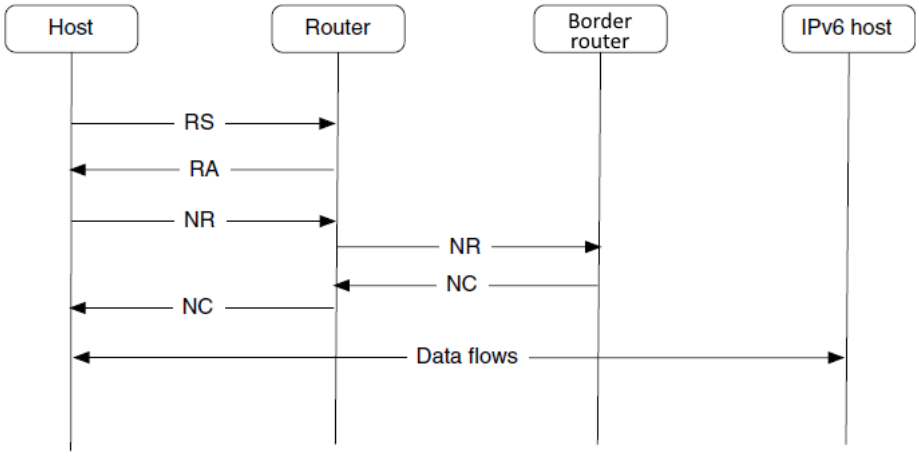

Figure 2.5.2: Multihop registration process with a border router.

assign.

2.6.2 Router operation

A LoWPAN router begins operations like any other LoWPAN node: it sets up its interfaces and their addresses, and carry out the detection of duplicate addresses required using the whiteboard, it must of first find the border router or other router that has a path to the border router.

Once the interfaces are implemented, the router can begin execution of the routing protocol is configured to use; once it has stabilized, it can advertise its services to other nodes using the periodic Router Advertisements and listening to Router Solicitations.

The network configuration settings that a router announces in Router Advertisements are copies of the ones it received during its own bootstrapping. As a result, these settings originate at the border routers. A router must continue to listen to Router Advertisements that it receives and update its settings whenever the sequence number in the 6LoWPAN prefix summary option increases.

The routers also manages the NCE (Neighbor Cache Entry) table where gathering all the addresses of LoWPAN network nodes. NCE can be of three types:

- *Garbage-collectible*: set according to the criteria given in RFC 4861 [54]. There among other current addresses DAD did not yet validated.
- *Registered*: valid with a period of lifetime.
- *Tentative*: temporary entry with a short lifetime, and which aims to pass Registered.

2.6.3 Border router operation

Most LoWPAN nodes have exactly an interface through which they run all their communications. The border router is different: it also has an interface to a larger IPv6 network, this can be backhaul link to some infrastructure unrelated to the LoWPAN, making a Simple LoWPAN, or it can be a backbone link connecting to other border routers in the same Extended LoWPAN. Obviously, the latter requires some coordination between the border routers.

The border router is a LoWPAN router, but with additional features:

- The border router is the source of the network parameters disseminated in the Router Advertisements, including the 6LoWPAN prefix and the other context entries for the context-based header compression. Generally, border routers will therefore require some configuration, while normal routers and hosts can bootstrap off the Router Advertisements, once commissioning parameters have been set.
- The border router has to run the whiteboard and the two conflict detection algorithms.
- The border router performs the routing from other IPv6 networks into and back out of the LoWPAN. To do this, it needs to run its other interfaces and possibly additional routing protocols over them. The border router also has some protection duties in performing this forwarding: it filters out certain ICMP messages to prevent Neighbor Discovery-based attacks, and it only forwards packets into the LoWPAN for addresses that have been registered

in the whiteboard, relieving the LoWPAN routing protocol from possibly expensively searching for a route to a node that does not exist. The system implementing the border router function may, of course, implement other protection functions, such as a firewall or other kinds of packet filtering.

2.7 Mobility and topology change

Many fields use mobile nodes with limited resources, moving from one place to another, like e-healthcare systems. The 6loWPAN WG has to deal with the mobility; both within the same LoWPAN network, or between two networks in two different areas. Mobility can be classified in two types: micro-mobility and macro-mobility.

2.7.1 Mobility types

Micro-mobility is the movement of the device in the same area of the network. In a 6LoWPAN, is the movement of the device in the LoWPAN network, with the same IPv6 prefix. An example is the node mobility and change its attachment from a border router to another in the same LoWPAN area. The node keep the same IPv6 address, and for the router that link border routers to the Internet, does not feel any change because nothing for it was change as long as the device maintains the same address. Inversally, macro-mobility is the movement of the device between two networks with two different areas, between two LoWPAN networks with different IPv6 prefix, which will change the node IPv6 address (fig. 2.7.1).

This is with regard to mobility for LoWPAN nodes, but if it concern to the movement of the total of nodes with the border router, we are talking about Network mobility. This may occur when moving the border router and its nodes, where it changes its IPv6 prefix. If we see the network mobility from the nodes side, we are talking about the macro-mobility because they will change their IPv6 addresses.

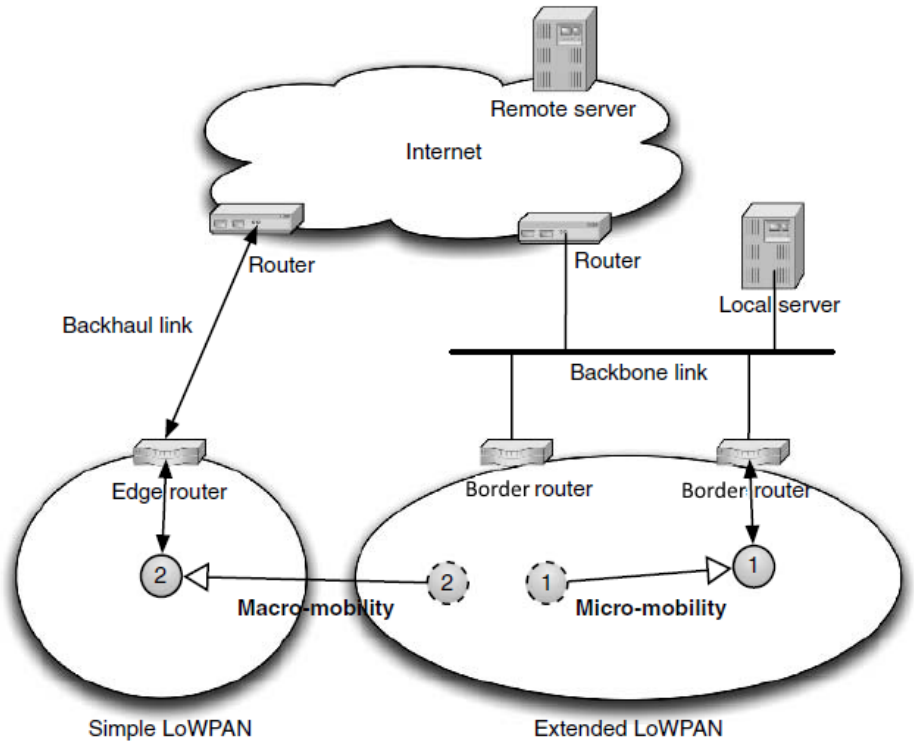

Figure 2.7.1: The difference between micro-mobility and macro-mobility.

2.7.2 Topology change

In wireless networks, there are several causes can change the network topology; we summarize in the following the principles topology change factors:

- *Physical movement*: when nodes physically move in relation to each other, the wireless connectivity between them change, so they change their point of attachment.
- *Network performance*: poor signal strength, overloaded channel capacity, node congestion or collisions because a high packet loss may oblige a node to change its point of attachment.
- *Radio channel*: changes in the network environment cause also changes in radio propagation; it is called fading. It often cause changes in topology even without physical movement, especially in the presence of simple radio technologies.
- *Node failure*: resource-constrained nodes tend to be prone to failure, for example due to battery depletion. The failure of a router will cause a topology change for the nodes that using it as their default router.
- *Sleep schedules*: battery powered nodes in low power wireless networks use long periods and frequent sleep schedules in order to save battery power. If a node finds itself attached to a sleeping router that does not have a suitable duty cycle for the application, this may oblige the node to move to another point of attachment.

2.7.3 Mobility solutions

In these cases, we must seek solutions to deal with changes. A set of proposed solutions was proposed:

- *MIPv6*: adapt Mobile IPv6 [89] for 6LoWPAN by compressing the headers and different messages.

- *Proxy Mobile IPv6*: use Proxy Mobile IPv6 [90] to overcome the problem of signage that cannot be managed by the nodes.
- *Lightweight NEMO*: a lightweight version of NEMO (Network Mobility) Basic Support Protocol [91] for 6LoWPAN whose aim is to reduce the overhead of the mobility by compressing it [92].
- *Inter-PAN*: a mechanism of mobility management at the 6LoWPAN adaptation layer [93].
- *Inter-Mobility*: a protocol that introduces new entities, 6LoWPAN PA (Proxy Agent). These PAs are responsible for the mobility management [94].
- *Inter-MARIO*: a protocol that has a managing handovers based on partner devices that detect the movement of mobile equipment and initiate the configuration. This speeds up the handover procedure [95].
- *SPMIPv6*: a protocol based on PMIPv6 (Proxy Mobile IPv6) that aims reduce energy consumption. Why mobility is managed by two new facilities; the SMAG (Sensor network-based Mobile Access Gateway) and the SLMA (Sensor network-based Localized Mobility Anchor) [96].

2.8 Routing

The 6LoWPAN routing scheme can be achieved in two different ways: mesh-under and route-over. Mesh-under is to implement a routing at the adaptation layer, while route-over realized this implementation at the network layer. In route-over, the IPv6 packet is reconstructed on each intermediate device to take the routing decision. In contrast, in mesh-under, the routing decision is done at the 6LoWPAN level and thus only with the fragments of the IPv6 packet. In this case, the IPv6 packet is reconstructed on the addressee equipment. As a result: mesh-under allows a shorter period of transmission; when route-over is more effective in degraded conditions (packet loss).

Regarding routing, 6LoWPAN network has introduced new concepts and measures that are not dealt by other standard routing protocols in wireless networks, such as AODV [97], OLSR [98], DYMO [99], DSR [100], etc. Studies [101], [102] showed that they are not well suited for LoWPAN networks as they consume more energy, they do not handle failure cases to establish a connection and they does not take on consideration nodes and links properties in establishing routes. Routers in LoWPAN networks uses only one wireless interface to forward packets from one node to its neighbor node, it ensures full connectivity between network nodes in forwarding packets via the same link through multi-hops toward nodes that are not accessible through a single wireless transmission.

2.8.1 The routing protocol: RPL

Routing protocols in LoWPAN networks have many constraints such as minimizing energy consumption, support nodes sleep cycles, consider the quality of service, support different types of addressing (unicast, multicast, anycast), support mobility, etc. All of that must be supported using a small amount of memory and bandwidth. A new IETF workgroup was created under the name of ROLL (Routing Over Low power and Lossy networks) to address general routing in LoWPAN networks and the requirements [103], [104] caused by the implementation of the new 6LoWPAN adaptation layer in these networks. The IETF-ROLL WG proposes the routing protocol RPL (Routing Protocol for Low power and lossy networks) introduced in the RFC 6550 [105], it is based on the distance-vector routing protocol algorithm. The distance-vector protocol considers that each router has a routing table indicating, for each destination network, the local interface to reach it and the best distance associated with it. The choice of using a distance vector algorithm is logical as the use of Link State algorithm is almost impossible in this kind of networks, Link State cost is very high in terms of computing and memory capacities since each state change, an update message should be distributed to all network nodes. This creates a huge traffic, especially in LoWPAN networks where the propagation conditions change the network status frequently.

2.8.2 RPL operation

The RPL protocol is based on the concept of DAG (Direct Acyclic Graph) to avoid creating loops in the tree constructed by distance vector algorithm. RPL has the ability to construct multiple paths back to the same destination and sets alternative routes whenever default routes are inaccessible. This protocol will target resource-constrained networks in terms of energy, power, bandwidth and a high probability of packets loss and a very significant error rate. RPL builds a DAG based on a root node called LBR (Low power and lossy Border Router), usually it is the border router 6LBR responsible for the management of a particular field of 6LoWPAN nodes and locate in junction of two networks. LBR, rank 1, is the source of the directed acyclic graph. This LBR and all upper level devices form a DODAG (Destination Object Directed Acyclic Graph), i.e. the construction of a DAG routed to a single destination. LBR sends an information message DIO (DOADAG Information Object) in multicast. When a device receives a new version of DIO, it calculates its particular rank (compared to the one it just received) and propagates its DIO. From the device point of view, all equipment having a lower rank can be parents. Optimal routes (parents) in the DAG are obtained from metrics and constraints. LBR periodically transmits DIO messages to update the DAG. When a device joins the network or loses the link to its "parents", it can wait for the next DIO (from a minute to an hour) or request a DIO the solicitation message DIS (DODAG Information Solicitation). DIO messages are sent with the Trickle algorithm. This algorithm mainly defines two things: a sequence number that indicates whether the received information is an update, and the delay between each information transmission (which varies depending on settings). These RPL control messages follow the format of the ICMPv6, which has a field in its header that defines the DIO message type (DAG metric container, Destination Prefix, DAG configuration), DAO or DIS. The concept that each node selects more than one "parent" node by DAG gives flexibility to RPL for self-healing by allowing it to adapt and overcome to topology changes. We obtain by RPL a topology in two forms: a hierarchical structure by the creation of the parent-child relationship between the

nodes, and the mesh topology by the possibility of routing between nodes of the same rank (fig. 2.8.1).

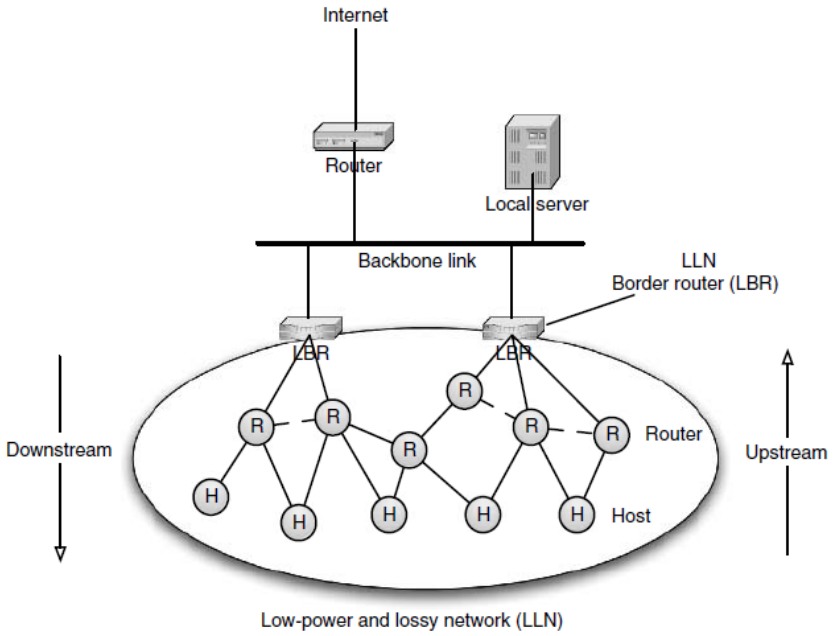

Figure 2.8.1: The RPL architecture.

2.8.3 RPL and Neighbor Discovery protocol

RPL can benefit from 6LoWPAN-ND protocol [53], the adapted version of the Neighbor Discovery protocol used by IPv6, responsible for the discovery of other hosts on the same link, determining their address and identifying present routers. The advantage of ND is that it provides useful information such as routing information on one-hop node, maintaining its cache information and maintaining routing information cache itself. This allows the RPL to have a self-configuration when needed. ND also helps RPL for the diffusion of its DIO messages across the network through the two allowed transmission directions: in the "downward" direction from the root to other nodes in broadcast transmission and in the opposite

direction the ”upward” from one node to the root in unicast transmission.

2.9 Integration to the Internet

By connecting a LoWPAN to the Internet or any other IP network, there are several aspects and issues to consider. 6LoWPAN simplify IPv6 requirements to allow it for for resource-constrained nodes over low-power wireless networks.

2.9.1 Application protocols

Application protocols on the Internet today, especially the Web part, depend on payloads of HTML (HyperText Markup Language), eXtensible Markup Language (XML) or Simple Object Access Protocol (SOAP) [106] carried over HyperText Transfer Protocol (HTTP) [76] and Transmission Control Protocol (TCP). This translates payloads ranging in size from a few hundred bytes to several kilobytes. It is too much to be used with resource-constrained nodes. It is preferably that end-to-end application protocols use UDP (User Datagram Protocol) and compact payload formats if possible. Technologies that are capable of transparent compression of web services in a format suitable for 6LoWPAN nodes are particularly interesting.

2.9.2 Maximum transmission unit

To comply with the IPv6 1280-byte MTU size requirement, 6LoWPAN performs fragmentation and reassembly operations. Applications designed for LoWPAN nodes should however try to minimize the packet size as many as possible, in order to avoid forcing IPv6 packets fragmentation because it affect network performance.

2.9.3 Firewalls and NATs

Firewalls and Network Address Translators (NAT) [107] are deployed in network everywhere. Many issues should be addressed when connecting 6LoWPAN via

them, for example blocking compressed UDP ports and non-standard application protocol used for 6LoWPAN applications.

2.9.4 IPv4 interconnectivity

6LoWPAN supports only IPv6, but since the majority of current devices use IPv4, there may be a 6LoWPAN node need to communicate with one of IPv4 hosts. There are several issues to enable IPv4 interconnectivity, including address translation IPv6-in-IPv4 tunneling. These mechanisms are usually located in the 6LBRs, on a local gateway or a node configured to do so on the Internet.

2.9.5 Security

When connecting LoWPAN devices to public Internet, security must be a major concern as they are limited in resources and are autonomous. The network limitations prevent the use of full IPsec suite, the transport layer security or the use of firewalls on each node. Even if data link layer use the IEEE 802.15.4 security insured by the AES 128-bit encryption provides some protection, but it not provides the end-to-end security.

2.10 Summary

The 6LoWPAN is a new technology in the world of the Internet and hence the interest in understanding its mechanisms before going to exploit it in the field of research. In the second chapter, we discussed 6LoWPAN mechanisms, requirements and challenges faced before analyzing all the proposed solutions to raise these challenges.

The IETF 6LoWPAN workgroup was convened to define the transmission of IPv6 packets on resource-constrained networks included in the IEEE 802.15.4 standard. The choice of IPv6 to enable LoWPAN devices to connect to the Internet was the result of several considerations and benefits. Devices with IP can connect directly to the Internet without using an intermediary or a gateway. In addition,

the Internet and everything that rotates around has been developed and used for years worldwide. However, despite all these advantages, the integration of IPv6 in devices with limited resources is not easy because of the many challenges, the currently available Internet protocols are designed for full resources devices and have not taken into account devices with limited resources. Many requirements are imposed by the nature of 802.15.4-based devices and other devices with limited resources. These requirements are not considered as a failure, but the nature of their operation imposed these characteristics. Most of these devices are wireless, capable of collecting and sending physical data detected in their environment, able to withstand very long time without any human intervention due to their low energy batteries, and thanks to their system that allows them to automatically interact with their environment and other neighboring devices.

The 6LoWPAN networks are created by connecting islands of wireless sensor devices, each island presents a stub network on the Internet. It is a network that IP packets are sent to or from its destination, but which does not act as a gateway to other networks. The 6LoWPAN architecture is made up of LoWPAN network(s). In order to get on a 6LoWPAN network, we must have a LoWPAN network that combines two types of resource-constrained nodes: host and router. The host device is the endpoint of the network, and a router acts as a link between the devices. This division of the devices came agree to the division of that it is in 802.15.4 standard that divides devices into two types: FFD (Full Function Device), and RFD (Reduced Function Device). These nodes communicate with each other through a wireless communication organizing in ad hoc, i.e. without having any infrastructure. They share the same IPv6 prefix. Regarding communication with other IP networks, it is established through the 6LoWPAN Border Router (6LBR). The 6LBR is a powerful machine, responsible for determining the IPv6 prefix and its distribution to the network nodes, assumes the role of the monitor and the controller of the LoWPAN, regulates sent or received packets traffic, supports compression operations of the header of the packet and manages Neighbor Discovery protocol operations.

The 6LoWPAN network topology may change due to several factors, among

them the moving nodes, since nodes can register in several LoWPAN simultaneously, which called multi-homing. The nodes may move throughout the LoWPAN between 6LBRs, and even between LoWPANs. Many fields use mobile nodes with limited resources, moving from one place to another, like e-healthcare systems.

Regarding routing, 6LoWPAN network has introduced new concepts and measures that are not dealt by other standard routing protocols in wireless networks. A new IETF workgroup was created under the name of ROLL (Routing Over Low power and Lossy networks) to address general routing in LoWPAN networks and the requirements caused by the implementation of the new 6LoWPAN adaptation layer in these networks. The IETF-ROLL WG proposes the routing protocol RPL (Routing Protocol for Low power and lossy networks) based on the concept of the DAG (Direct Acyclic Graph) to avoid creating loops in the tree constructed by the distance vector algorithm. RPL has the ability to construct multiple paths back to the same destination and sets alternative routes whenever default routes are inaccessible. This protocol is designed especially for resource-constrained networks.

Like any new technology, several issues and challenges confronted. First comes the security as the main challenge. The application of a technology in the field of healthcare often was limited by privacy concerns, the "medical secret". The next chapter will focus on security in 6LoWPAN networks, which we will address the following questions: What are the threats to the security of 6LoWPAN network ? What are the available options ? Are they compatible with this type of network ? What is the appropriate proposal to solve the security issues ?

History has taught us: never underestimate the amount of money, time, and effort someone will expend to thwart a security system. It's always better to assume the worst. Assume your adversaries are better than they are. Assume science and technology will soon be able to do things they cannot yet. Give yourself a margin for error. Give yourself more security than you need today. When the unexpected happens, you'll be glad you did.

Bruce Schneier

3

6LoWPAN security analysis

Because of the sensitive roles that a sensor may play in an e-healthcare system by sending accurate and private information, we must think of means of the protection of information and the protection of the network as whole. In 6LoWPAN network, it will be more complicated as a device is no longer circulating data with other devices present in its network. By its integration to the Internet, the device will become within the scope of a global network of devices of all varieties. It can be exposed to attacks from anywhere in the world. As well as its presence in hostile environments, it makes it vulnerable to be compromised and used as a tool of an attack. Security in 6LoWPAN networks is a sensitive and essential element that we must deal with all its sides.

3.1 Preamble

One of the most important aspects to be taken into account when creating a 6LoWPAN network is setting the security mechanisms and maintain it. 6LoWPAN networks are inherently open to the attackers whose can eavesdrop the information exchanged within the network, or injecting false packets into it.

It makes it more complicated the impossibility of application of current security systems used in today's networks, for several reasons, being limited resources and high consumption of energy, making it difficult to provide the protection systems of complex computations, which need high-performance resources and consume a lot of energy. Any proposal to resolve the terms of the security of 6loWPAN network must take into account two factors; the need to use limited resources and the need for minimal consumption of energy, any proposal that consumes a lot of energy will be ineffective and sentenced to failure.

The possibility of capturing 6LoWPAN devices is another complicated problem. Because of their small size and their location in insecure places, an attacker can steal their data, re-programmed and re-integrated them in the network as an intruder device to eavesdrop data or to harm the network. The eavesdropping process can be carried out via the shown way, or through a powerful machine that can pick up devices signal, or even remotely via the Internet. There are many forms of attacks and threats we will treat it in detail in the following sections. Generally, it aims to introduce false information affecting the cost-effectiveness and quality of the network, or to tamper the functioning of the full network as a whole or a part of them as Denial of Service attacks. Attacks can be done via a malicious node, a powerful machine placed approximately to the LoWPAN, or remotely through the Internet.

Adding to the complexity, the difference between networks topologies, the change of their characteristics and the security needs that differ from a domain to another. Since the 6LoWPAN networks share many properties with MANET and WSN networks, therefore the possibility of applying security solutions for these two networks on the 6LoWPAN network. However, that would not work, since

the proposed solutions for MANET are designed for powerful machines and did not take into account devices with limited resources, and WSN solutions are not sufficient, as they do not provide the end-to-end communications security with external devices.

The challenge that we will deal with it to secure the 6loWPAN networks is how to find an appropriate solution that takes into account of these characteristics and constraints, by raising the level of security with no large consumption of resources.

3.2 Security objectives

Any information system cannot be accepted or marketed if it not provides security, at least its most important objectives: confidentiality, integrity, availability, authentication, freshness, resiliency, and end-to-end security in the Internet context.

3.2.1 Confidentiality

It mean that is not possible to read data from a non-authorized party. Done by encrypting data, no one could understand it content, only authorized parties that have the mechanism of decrypting it. Everything will get the eavesdropper is a set of symbols with no meaning and cannot deduce which is its real content.

3.2.2 Integrity

The device should receive the data as is expected, and cannot change it by a non-authorized person. When the exchange of data between two authorized devices, as it is sent from the first party, it must reach out the second party also sent accurately, even if it is passed through several other interface devices. Encryption alone does not guarantee the integrity of the information; other mechanisms must be added to check the integrity.

3.2.3 Availability

The device system and applications must be available during times of expected use with a reasonable answer time. We can say for that the device will be available; it must be protected from Denial of Service attacks.

3.2.4 Authentication

Confirm the identity of the sender and verify that it is an authorized device, in order to create trust between the devices with each other, and restricting the exchange of data between only authorized devices without the intervention of extraneous and undesirable ones.

3.2.5 Freshness

Check for data freshness, i.e. it is not replayed from outdated information. Some of the attackers have recourse to re-send correct information posted by an authorized device, in order to charge the network and exhaust the device energy. If we did not consider this, the device will deal the same data every time it reaches out, as the data being correct, safe and reliable.

3.2.6 Resiliency

Continuing to provide an acceptable level of security, even if a part of the network crashes, in the presence of compromised or captured devices. Any system must not depend on a security system; if it is breached, it will lead to the collapse of the entire network.

3.2.7 End-to-end security

In addition to the protection requirements common to all systems and networks, there is another requirement to protect must be supplied to the 6loWPAN networks, being the networks rely on the IP communication, a system of "end-to-end" security.

We can be resorting to all mentioned security requirements or some of them, depending on the application requirements, which vary from a field to another. For example, we can dispense with the requirement of privacy in the network that provide public information, but in our e-healthcare applications; it is indispensable. It is difficult to provide a security system that works well in all the networks topologies. However, we are providing a range of mechanisms of which are used as needed, and remain the responsibility of ways of governance, management and maintenance that must be adapted to the requirements of each application and the environment in where it will be applied.

3.3 Threats and vulnerabilities

Since 6LoWPAN is a combination of two systems (IPv6 and IEEE 802.15.4), in this section we analyze the different possible threats and vulnerabilities from the two sides that target all layers of the 6LoWPAN stack.

The specific features of LoWPAN networks (limited energy, low-power computing, wireless communication, etc.) expose 6LoWPAN nodes to many threats. While some of these threats can be found in all ad hoc networks, others are specific to this type of network and is designed specifically to address the limited energy of sensors. In cases of attacks found in LoWPANs networks, an attacker can attempt to retrieve information from the network by listening to the medium, if the network does not encrypt data. In this case, we talk about passive attack, the attacker seeking here to eavesdrop and retrieve information.

In the case where the attacker tries to modify or delete information, or even to prevent the network to function properly, we talk about active attack.

These attacks occur through compromised nodes presents itself as an authorized node, or extraneous devices contain the same security mechanisms of authorized nodes. If the attack is done by the same device capabilities of LoWPAN nodes, i.e. with limited resources, the damages do not exceed its surroundings and its neighboring devices. However, it is not the case all the time as the attack can be done directly from the nearby LoWPAN entourage, by powerful devices bearing

strong processors, high-energy, with high bandwidth and strong radio transmitter.

3.3.1 Threat model

When we define the security objectives, we need to understand the threat model: what is the attacker will be able to do that can work against the security objectives. An important sub-question that we should deal with it to understand the intention of the attacker is the level of benefits that he may obtain from subverting a security objective. This can affect the amount of resources that the attacker can deploy.

In the wireless systems as 6LoWPAN, the threat model is not very different from the model assumed for Internet security protocols; the Dolev-Yao model [108]. The attacker is assumed to have a quasi-complete control on the communication channel. He has the ability to read any message, even delete it or modify it. He can also inject new messages, because without cryptography, there is no way to protect messages to be read, or to detect a message that has been altered.

Internet threat model assumes that the end devices were not be compromised, because it is very difficult to maintain total security if this assumption cannot be made. However, the distributed nature of the LoWPAN nodes and their small size creates a significant threat in many LoWPAN deployments, it will be easy to get a node physically and control it even remotely; the low cost requirement will limit the degree to which nodes can be made inviolable. Yet, measures should be taken to limit this damage.

In particular, it is a further important requirement that the protection of the whole network is not dependent on the memory integrity and confidentiality, of each single node. This creates difficult problems, it is important to find a balance between the potential damage and the cost of maintaining security.

In our case, the architecture of an e-healthcare system may vary depending many requirements and constraints, but generally the system is composed by three major component; the wireless body sensors, the Medical Central Unit and the gateway that links the sensors by the Internet that may be a router, PDA, smartphone, etc.

We assume that both the gateway and the Medical Central Unit are secure and

trustworthy, as they are full resources devices; implemented by the performant security protocols.

We assume an ideal network where no exchanged message is lost and all of them are sent and received instantly by the communicated devices. Moreover, all communication channels are assumed public.

The attacker cannot intervene by an active attack by capturing or compromising a node in the bootstrapping phase during the network deployment, but he can execute a passive attack like eavesdropping the flow between the wireless sensors and the gateway in this phase. Thus, it is not possible to take into account the time that the attacker make to execute its attacks.

If the attacker compromise a node, he can reveal the key stored in it, but it will obtain only the key of the current session. He can encrypt and decrypt messages by the key in his possession and he is capable of storing, deleting, build and send all the messages with this key.

We assume the used cryptography, even the symmetric or the asymmetric, is perfect. Encrypted messages can only be read if the decryption key is available in the node.

Since 6LoWPAN consists of two networks, IPv6 network and 802.15.4 network, it will be targeted by their security threats. Therefore, we must deal with these threats at these levels taking into account the new features added by the 6LoWPAN technology.

Threats in the LoWPAN networks are divided into several types. It can be divided from the point of view of the attack, whether it is an internal attack by a device within the network, or external attack by a machine outside the network. It can be divided according to the type of the attack, whether it is a negative attack that its goal is eavesdropping data without making any damage, or an active attack that aim tampering the network and damaging devices.

3.3.2 Threats on the IEEE 802.15.4 side

The security threats in LoWPAN networks have been widely studied by the scientific community. Attacks can be classified by several regimes: outsider-insider, unfavorable sources, passive-active methods, compromise, host-based or network attacks [109].

From the perspective of the security from any threat, detecting external and insider attacks requires different systems of protection. The attackers outside the network can launch passive attacks such as unauthorized listening or active attack like Denial of Service (DoS). The defense system normally uses cryptographic mechanisms to prevent or eliminate foreigners to join the network, but malicious insider nodes can be created in several ways: attackers physically capture nodes and reprogram them, or they use software and devices to breach key cryptography or inject malicious code [110]. In these cases, the attackers have all the keys, so they can easily overcome any test of cryptography. Insider attacks are generally aimed at destroying a network operation, it is better to implement a surveillance system well specified, which can discover early any network behavior anomaly.

Outsiders and insiders attacks are applied to all LoWPAN layers. Some threats are more dangerous because they can be easily deployed and can generate complex attacks. If the system cannot identify them early, their effects on the functioning of the network can be very serious in both short term and long term. Some of them can make the LoWPAN unavailable, partitioned or resource exhausted. In addition, when applying mechanisms such as IPv6 Neighbor Discovery and address autoconfiguration in LoWPAN there are Neighbor Discovery threats as described in RFC 3756 [111]. If the attackers crack these mechanisms to usurp the Neighbor Solicitation / Advertising or redirect messages, they can degrade performance by falsifying routing topology view of the members.

As can be seen, some attacks target the data confidentiality and others aims at degrading the network operation. Therefore, it is necessary to specify and deploy a cryptographic system to protect nodes data, and an intrusion detection system for monitoring the network performance to detect abnormal behaviors of malicious

nodes.

3.3.3 Threats on the IPv6 side

End users from the Internet can access information from the node field once 6LoWPAN is implemented. This increase the threat of authenticating from users and nodes, user accountability and the network availability. The attacker can illegally access the information if no authentication mechanism is applied in the network. When a channel of communication between the end user and the LoWPAN network is established, the attacker can eavesdrop sensitive information from the data stream, which breaks the integrity of the network. Furthermore, the responsibility of users accessing the network should be considered to detect and recreate security incidents [112]. The availability of communication must be guaranteed by the protection of the LoWPAN nodes.

Another type of threat is that an attacker from the Internet can take control of the LoWPAN nodes. This kind of attacks alters the end user data, which leads to false information and decision. Also, the outsider attackers can launch DoS attacks by flooding to drain the power of the node.

A line of cryptography must be implemented to protect the confidentiality and the integrity of the exchanged data between the end users, but cryptography only cannot defend itself against DoS attacks from the Internet to the sensor network, so it is necessary for the implementation of an intrusion detection system (IDS) to analyze IP traffic between the two. In addition, in the traditional Internet IDS solutions or in the sensor array cannot simply be applied because of the different nature of these two traffic network designs.

3.4 Taxonomy of attacks

Most of the attacks against 6LoWPAN networks can be devastating, because of the nature of the devices and the constraints of their properties, especially with regard to energy and batteries vulnerable shipping, as well as the processor, memory, wireless radio, put them in hostile places and make it part of the giant Internet

and filled with risks and threats. In the case of an e-healthcare system, it poses a direct threat and risks to the health and lives of people. Among the most serious and easiest threats is the risk of DoS attacks. They aim to make a node or a network unavailable for a certain period. The general principle of DoS attacks is sending data or packets whose size or content is unusual to cause unexpected reactions of the network or targeted node, sometimes they can even cause the service interruption. This kind of attack is very common on networks because it is simple to implement and can nevertheless have devastating consequences. In addition, the detection and prevention of these attacks are very difficult because they can take many forms.

The basic attacks type are whose targeting the consumption of the bandwidth, the consumption of the processor time or the memory storage ability, creating a congestion in communication links between nodes, the disruption of a component, a service, a routing information or all the system, etc., the 6LoWPAN resource constraints make its routing protocol vulnerable to DoS attacks and easy to disrupt.

3.4.1 Physical layer

Physical Layer is responsible for the actual data transmission and reception, frequency selection, the generation of the carrier frequency, and the signaling function of data encryption. This layer also covers the transmission media between communication nodes. LoWPAN uses a shared radio transmission medium based, which makes it vulnerable to jamming or radio interference.

3.4.1.1 Jamming

The medium for transmitting information is a vulnerable point in a network. In this case, it is almost impossible to restrict access to a medium using radio signal. An attacker can therefore send signals in the same frequency as the LoWPAN nodes to scramble radio signals. Network nodes then do not have access to the medium and cannot communicate because of this radio interference. This leads to an isolation

of the nodes as the jamming signal continues to propagate. No message can be exchanged between the affected nodes and other nodes.

3.4.1.2 Tampering

A malicious node will retrieve a message and alters it by adding false information, by modifying or destroying packages to make it an incomprehensible information. The node can be converted to a malicious node controlled by an attacker by altering or replacing it.

3.4.2 Data link Layer

The data link layer provides the movement of the frames from hop to hop, the physical transmission of data streams, the media access control, network topology, detection of data frames and error control. Attacks at this layer include resource exhaustion purposefully created collisions, and unfairness in allocation.

3.4.2.1 Collisions

A data collision occurs when two nodes of the same or different networks attempt to transmit on the same frequency at the same time. When packets collide, they are rejected and must be resubmitted. An opponent can cause collisions strategically in specific packages such as ACK control messages. The adversary can tamper the communication protocol by transmitting messages continuously in order to generate collisions.

3.4.2.2 Exhaustion

Resource exhaustion is caused by an attacker using repeated collisions. For example, an implementation in data link layer may continually retransmit corrupt packets. Unless these desperate retransmissions are discovered or avoided, the energy of the transmitting node and those around reserves will be depleted quickly.

3.4.2.3 Unfairness

Unfairness can be caused by an adversary using the above data link layer attacks. The attacker aims to disrupt the other nodes' frame transmissions by causing degradation of real-time applications.

3.4.3 Adaptation (6LoWPAN) layer

The adaptation layer is used at the border router 6LBR in order to translate the packet between the two networks: IPv6 network and LoWPAN network. The 6LBR is normally a wired node and has a high security protection. However, packet fragmentation and reassembly progress still have some vulnerability.

3.4.3.1 Fragment duplication

The fragment duplication attack leverages the fact that a recipient cannot verify at the 6LoWPAN layer if a fragment originates from the same source as previously received fragments of the same IPv6 packet. Thus, the recipient cannot distinguish legitimate fragments from spoofed duplicates at the time of reception. Instead, it has to process all fragments that appear to belong to the same IPv6 packet according to the sender's MAC address and the 6LoWPAN datagram tag.

3.4.3.2 Buffer reservation

The buffer reservation attack targets the scarce memory of resource-constrained nodes and leverages the fact that the recipient of a fragmented packet cannot determine a priori if all fragments will be received correctly. Hence, a receiving node must optimistically reserve buffer space for the reassembly of the complete packet as indicated in the 6LoWPAN header. Other fragmented packets are dropped by the recipient if the reassembly buffer is already occupied. As the buffer reservation attack affects an individual reassembly buffer, the effort for an attacker to mount this attack grows linearly with the number of buffers at the target node.

3.4.3.3 IP fragmentation

Some fragmentation attack techniques of the IP network can be applied in this layer by modifying or rebuilding the packet fragmentation fields, such as datagram size, datagram offset or datagram tag. Examples of threats are tiny fragmentation, Ping of Death, Jolt, Teardrop, New Teardrop, or Router Frag attack. These attacks can cause critical damage to a sensor node, for example, back buffer overflow due to packet re-sequencing, exhausting the resources due to the processing of unnecessary fragmentation, or stopping and restarting.

3.4.4 Network layer

The network layer is responsible for intra-network operation, addressing nodes management, tracking the location of devices and finding the most effective way for the packet to travel on the road to a destination. It manages data routing and transmission from the 6LBR to the nodes and vice versa.

3.4.4.1 Replay

Replay attack is the most common direct attack targeting the network layer routing protocols. It targets the exchanged routing information between the nodes. If packets sent over the network, it can be read and recorded by an attacker; it may return these packets later to fool the network.

This attack is feasible if the package did not contain information regarding the date of shipment, or if that date is accessible and easily alterable by an attacker.

Attackers may create routing loops, repel or attract network traffic, shorten or extend source routes, generate false error messages, increase the latency from end-to-end and partition the network.

3.4.4.2 Sinkhole

In this attack, a malicious node will directly address the information flowing from and to the 6LBR. For this, the malicious node will offer network nodes the fastest

path to reach the base, using for example a more powerful connection. So all of these nodes will address in particular the malicious node to transmit information to the base. The attacker will recover any information that flows from these nodes to the base node.

The main reason why 6LoWPAN networks are sensitive to sinkhole attacks is due to their specific mode of communication. It can be very difficult for an attacker to apply this attack in a network where each pair of neighboring nodes uses a unique key to initialize spread spectrum or frequency hopping communication.

3.4.4.3 Hello flood

Discovery protocols on ad-hoc networks use HELLO messages to fit into such a network and discover its neighboring nodes. In a so-called Hello Flood attack, an attacker will use this mechanism to use energy sensors and prevent their messages from being routed.

An example of a malicious node with a powerful radio connection that allows it to send a large number of HELLO messages, continuously. The nodes will then consider the malicious node as a neighbor, even if they are located at far distances from it.

When they try to send data, these nodes will pass through the malicious node they consider their neighbor, but their messages will never reach it. Since this node is inaccessible, they will use their radio antenna at full power, while consuming their energy and their messages will be lost.

3.4.4.4 Blackhole

Blackhole attack is performed by a malicious node in the network, which by various means, will modify the routing tables to force the maximum neighboring nodes to route their information through it. Then like a black hole in space, all the information within it go past will never be retransmitted. In this case, the blackhole will broadcast any information, preventing communication between the network nodes.

3.4.4.5 Sybil

A Sybil attack is that a malicious node masquerading as multiple nodes using the identity of other legitimate LoWPAN nodes. The Sybil attack will then be able to try to undermine the mechanisms such as data aggregation, security, routing, resource allocation or intruder detection.

In a cluster topology, a malicious node can impersonate more nodes and gain a significant advantage in an election of cluster head. With a greater number of votes, it can deceive its neighbor nodes to the cluster, for example, encourage the elected as clusterhead. If the malicious node gets this distinction, its decisions within the cluster will have a greater impact (refusal routing information outside the cluster, sending truncated information on neighboring clusters, etc.).

3.4.4.6 Wormhole

The attack of the wormhole requires insertion into the LoWPAN at least two malicious nodes. These two nodes are connected together by a strong connection can be wired or radio. The purpose of this attack is to trick the neighboring nodes on the distances separating them. Generally, the routing protocol seeks the shortest path in number of hops. In the case of an attack of the wormhole, both malicious nodes can achieve a remote location in a single hop.

This possibility will deceive other nodes on the actual distances between two nodes, but will mainly have the effect that the neighboring nodes will mainly go through these malicious nodes to circulate their information. Moreover, malicious nodes that form the wormhole will be in a privileged position that will allow them to have priority over the information flowing through their neighboring nodes.

3.4.4.7 Acknowledgement spoofing

Several routing algorithms for LoWPAN networks based on acknowledgment of the implicit or explicit link layer. Protocols that choose the next hop based reliability issues are susceptible to this attack. An attacker can spoof acknowledgments

link layer for packets addressed to overheard neighboring nodes because of the inherent broadcast medium. This results in packets being lost when traveling along these links. Its goal is to convince the sender that a dead or disabled node is alive or the weak link is strong. Since packets sent along weak or dead links are lost.

3.4.4.8 Internet smurf

The Internet smurf is a Denial of Service attack in which a large number of ICMP packets with spoofed source IP address of the intended victim are diffused to the network nodes using an IP broadcast address. Most of these nodes will answer by sending a reply to the IP address source. If the number of the network devices that receive and respond to these packets is a lot, the victim node will be flooded with traffic.

3.4.4.9 Selective forwarding

Multihop communication method is often preferred in the protocols for data collection in LoWPAN networks. Multihop networks assume that participating nodes will faithfully receive and forward messages. Yet, a malicious node can refuse to forward some packets and simply drop them, ensuring that they do not spread further. An adversary node selectively transmits some packets while dropping others. In another scenario, an adversary can selectively deposit original packets from a source and transmit the others.

3.4.4.10 Sniffing

Sniffing attack is an attack that involves passive monitoring and network monitoring mechanisms. The attacker by analyzing only the paths taken by packets on the network can retrieve valuable information about vulnerabilities in the network. Traffic analysis can allow an attacker to know the position of the nodes of data aggregation or network databases by identifying areas where the largest number of packets in transit. This type of attack does not affect the normal operation of the

protocol. An external attacker can launch this attack to collect valuable data from the LoWPAN nodes.

3.4.5 Transport Layer

End-to-end connections are managed in the transport layer. It provides a service for sending and receiving data from the LoWPAN node connected to the Internet.

3.4.5.1 Flooding

A protocol is vulnerable to memory exhaustion flooding whenever it needs to keep the state at each end of the connection. An attacker can request repeatedly new connection until the resources required by each connection achieve maximum limit and become unavailable. In both cases, other requests will be ignored.

3.4.5.2 De-synchronization

De-synchronization is the disruption of an existing connection. An attacker may spoof messages repeatedly to an end host for that this host become obliged to request the retransmission of lost frames. If timed correctly, an attacker can degrade or even prevent the ability of end hosts to exchange data successfully giving way to waste energy trying to correct the mistakes that never really existed.

3.4.6 Application layer

The application layer is responsible for submitting all information necessary for the application and spread of requests the application layer to the lower layers. It contains the element of service to support the implementation process such as data collection, management and processing of data through the application software to obtain reliable results.

Most sensor networks are deployed in hostile environments, which do not allow a human monitoring of all sensors. Then it is quite possible for an adversary to physically attack a sensor to compromise. This physical attack can allow an attacker

to extract cryptographic keys stored in the sensor or modify the program in it to replace it with another, so that the sensor becomes what is called a compromised node. This compromised node controlled by the attacker will allow it to integrate into the network to retrieve information or launch other attacks from that node or more of these nodes as described in the previous attacks. Some recent research aim to create resistant sensors to physical attacks with mechanisms such as deleting cryptographic keys upon detection of a physical attack sensor. A summary of this attacks classified according to the network layers is given in the Table 3.4.1.

Layer	Attacks
Physical layer	Jamming Tampering
Data link layer	Collisions Exhaustion Unfairness
Adaptation layer	Fragment duplication Buffer reservation IP fragmentation
Network layer	Replay Sinkhole Hello flood Blackhole Sybil Wormhole Acknowledgement spoofing Internet smurf Selective forwarding Sniffing
Transport layer	Flooding De-synchronization
Adaptation layer	Tampering attack

Table 3.4.1: Layering-based attacks.

3.5 Cryptography

In most current security mechanisms, cryptography is probably the most used technique. Data encryption prevents eavesdropping data transmitted over a wireless network and ensure data confidentiality.

As part of wired networks and traditional wireless networks owning important computing capacity and significant memory, the encryption solutions are considered as safe solutions that address all issues related to data security. The specifics of LoWPAN networks, namely a low computing power and limited memory that is added the problem of energy conservation, are significant barriers to the use of current cryptographic systems deemed safe and secure (SSL [113], RSA [114], etc.).

The current research focus on finding so-called lightweight cryptography solutions. These solutions consist in adapting traditional cryptographic algorithms for LoWPAN networks, or finding new ones just as effective in terms of security, execution time and energy consumption. These solutions are of two types of cryptography: symmetric cryptography and asymmetric cryptography, commonly called public key cryptography.

3.5.1 Symmetric Key Cryptography

The principle of symmetric cryptography is based on sharing the same encryption key K between two entities, A and B. If A wants to communicate a message to B, A will encrypt the message M with the key K, then transmits its M_K encrypted message to B over the network. This message cannot be decrypted without the key K, which ensures confidentiality. When B receives the M_K message, it decrypts the message M with the encryption key K. The symmetric cryptographic algorithms are divided into two subsets, stream cipher and block cipher algorithms.

3.5.1.1 Stream cipher

For stream cipher, the technique used is to encrypt the message to be transmitted after performing an XOR with the encryption key. Let M be the message to be encrypted, the encryption key K, and the Boolean XOR operation $\oplus$, the encryption is:

$$M \oplus K = M_K \tag{3.1}$$

Where M_K is the encrypted message.

Decryption then done by:

$$M_K \oplus K = M \oplus K \oplus K = M \tag{3.2}$$

This technique of stream ciphers is that used by the algorithm RC4 for example.

3.5.1.2 Block cipher

The block cipher consists of cutting a message M into blocks of n bits, these blocks will then be encrypted using a function f and a key k derived from a master key K.

Let M be the message to be encrypted cut into r blocks of n bits, K is the encryption key that are extracted the key k_i and the encryption function f.

For each block b_x of M, encryption will be as follows:

$$C_1 = f(k_1; b_x) \tag{3.3}$$

f is then iterated a number y of times therein extracted with a new master key K, called iteration round and which guarantees the security of the encryption algorithm, thus:

$$C_2 = \oint(k_2; C_1) \tag{3.4}$$

$$C_y = \oint(k_y; C_{y-1}) \tag{3.5}$$

The decryption is done with an inverse function G of the function F and the different shared key K obtained from the common key K, as follows:

$$C_{y-1} = G(k_y; C_y) \tag{3.6}$$

so

$$C_{y-1} = G(k_y; \oint(k_y; C_{y-1}) \tag{3.7}$$

$$b_x = G(k_1; C_1) \tag{3.8}$$

The block cipher is the most common symmetric cryptography technique, used by the cryptographic algorithms such as DES [115], AES or Blowfish [116]. Where AES 128 is deemed secure by a number of rounds equal to 10, below the existing attacks that break the encryption proven by a number of rounds equal to 7.

However, if the symmetric key encryption is possible in LoWPAN networks, the overall security of this type of solution remains to be seen. On the one hand because the only symmetric key encryption does not guarantee data authentication as can the digital signature public key ciphers, and secondly because there is the problem of the distribution of encryption keys. Therefore, if the IEEE 802.15.4 protocol specifies the encryption method to be used at any time; it does not specify how the keys should be managed and how to enable authentication of data.

From this perspective, typically we found different solutions to this problem. Each of the following solutions meets a different need based on the type of applications for which a LoWPAN network is deployed (information retrieval only by the base, collaborative exchange of data between sensors, etc.).

The four main key distribution solutions are network key, pairwise key, cluster key and individual key.

3.5.1.3 Network Key

It is a shared key by the entire network. To send a message, the information is encrypted with this key. Once the message is received, it can be decrypted with the same key (the principle of symmetric key). This solution is one of the less expensive energy cryptography solution, because the data is encrypted by the transmitter only once and decrypted only once by the receiver (usually the base station). Moreover, this solution solves part of the problem of passive listening, because the information is no longer circulating in the clear. However, if an attacker could find the key, he is able to listen to the entire network that communicates only with this unique key. Knowledge of this key also allows it to have the ability to insert a malicious node in the network.

3.5.1.4 Pairwise key

Each node has a different key to communicate with a neighboring node that shares this key. Therefore, if a node has n neighbors, it has to store n keys to communicate with its neighbors. In this solution, a node that wants to send a message must be encrypted with the neighbor key who receive this message. The neighboring node will decrypt the information for re-encrypt by the key corresponds to the next recipient. This solution can significantly increase network security as a key discovery makes it possible to communicate with two nodes, and reduces the attacker damage. However, this technique is very costly in energy and especially in computation time because each pair of nodes that transmit the information must perform the encryption and decryption operation. Which will reduce the lifetime of the network as well as its fastness.

3.5.1.5 Cluster key

In this case, each group or cluster of nodes share a common key that allows them to communicate within the group. The cluster head nodes communicates within them by a common key, or by a pairwise key. This solution is a hybrid of the first and second encryption techniques. It reduces the number of communications in encryptions. However, it has to default to charge the cluster heads by the encryption operations. To remain effective, we should make sure to change regularly the cluster head node within a group to do not consume all the energy of this node.

3.5.1.6 Individual key

In this solution, each node has a personal key to encrypt its data. This key is known only to the base station. A message sent by this node circulate on the network as hidden until it reaches the base station. This solution is one of the best techniques to limit consumption of the network. However, it does not allow securing information transmitted between the nodes, as they have no encryption key to secure communication between them.

3.5.2 Public Key Cryptography

The asymmetric key cryptography, more commonly known as public key cryptography, is considered more secure than symmetric cryptography because it allows, via the digital signature, to authenticate the sender.

The public key cryptography is based on the use of two keys, a private key K_p guarded secretes by its owner and a public key K_P broadcasted by its owner to enable devices wishing to provide to it their data encrypt their message with the public key K_P.

The public key cryptography is based on the principle of one-way function. Moreover, a message encrypted with the B public key K_P cannot be decrypted with the same key. It is decipherable only by the owner of the private key K_p namely A. Thus guaranteeing to B the sender of the message encrypted with the public key of A that only A can decrypt the message.

Formally, the data encryption and decryption of a message between two devices A and B corresponds to the following mechanism:

K_P is the public key and the K_p the private key of A, f is the encryption function and G the decryption function. A broadcasts its public key in the network. Let M the message that B wants to transmit to A, then:

$$M_k = f(K_P, M) \tag{3.9}$$

where M_k is the encrypted message.

and

$$M \neq G(K_P; M_k) \tag{3.10}$$

B sends the message to A that will then be able to decrypt it with its private key:

$$M = G(K_p; M_k) \tag{3.11}$$

Moreover, B can ask A to prove its identity with the mechanism of the digital signature. For that, A will encrypt a message with its private key, B will then decrypt the message with A's public key. Since only A has the private key corresponding to the public key, if the message can be decrypted with the public key, B is normally assured that the message actually comes from A.

Public cryptography mechanisms are potentially good solutions for security by providing a share confidential data and secondly the authentication mechanism. However, the need of processor power to execute its algorithms makes it more complicated than symmetric encryption algorithms. This type of cryptography is not suitable for LoWPAN networks.

3.6 Key establishment schemes

As said in the previous section, the cryptography need a protocol for initial key establishment that must be adapted to 6LoWPAN resource-constrained devices.

Even if many key establishment protocols exit in today's Internet, but the underlying cryptographic algorithms are too complex and heavy to implement in this kinds of devices. Key establishment protocols provide a shared secret between two nodes or more.

Key establishment protocols are classified according to four criteria:

- *Key delivery scheme*: key agreement or key transport.
- *Underlying cryptographic primitives family*: asymmetric or symmetric.
- *Authentication method*.
- *Involved peers number*: peer-to-peer, three or more, server-assisted.

We discuss these criteria in the following paragraphs.

3.6.1 Key transport vs. key agreement

A two-party key transport protocol is a protocol that operates between two peers, where one or more secret values are generated at both peers or at one of them and transferred securely to the other thereafter. The resulting key is created from transferred secret values with the possibility of using other parameters that may have been exchanged in the key transport.

In a one-pass key exchange, a single secret value is sent from one peer to another. The key can be derived from this secret value itself, or from it as well as other parameters. In a two-pass key exchange, the two peers exchange secret values that are used as input to the function of key generation.

A server-assisted key transport is used for the distribution of a session key from a central server called KDC (Key Distribution Center) to two peers. This requires that the KDC be capable of distributing a key in a secure manner, for example, by pre-established secure channel for the two peers. Another variety less frequent is the server that allow one peer to generate the session key, get it from this peer, and transmit it the other peer through a secure tunnel. In the second variety, the assistance server is called a KTC (Key Translation Center).

A two party key agreement protocol is a protocol that operates between two peers, wherein the resulting key is derived from two pairs of public information exchanged between these peers. The public information can take the form of an encrypted secret.

3.6.1.1 Diffie-Hellman protocol

The Diffie-Hellman (DH) protocol [117] is the most widely used key agreement protocol and best known. The Diffie-Hellman key exchange process allows two parties to agree on an encryption key without having to worry about the confidentiality of this exchange.

It is based on the existence of functions, called one-way functions that are characterized by the fact that the calculation is in one direction (encryption) and almost impossible in the other (decryption, and so the attack by a cryptanalyst) without the knowledge of a private key.

It requires that both peers A and B agree firstly on appropriate prime (p) and generator (g). The process is the following:

Both parties A and B share two non-secrets parameters: a prime p and a primitive root of p, i.e. a number g whose modulo powers p generate Z_p - 0.

Each one chooses a private key in the interval [1,. . , p-2], A choosing a value a and B a value b.

Each computes a public value that is exchanged:

A sends $\alpha = (g^a \ mod \ p)$ to B, and B sends $\beta = (g^b \ mod \ p)$ to A.

A calculates $\beta^a \ mod \ p$ and B calculates $a^b \ mod \ p$.

This value is necessarily the same, they have a value k that acts as shared secret key[1].

Suppose for example, A and B share p= 233 and g = 45:

if A chooses a = 11 and B b = 20, then

$\alpha = 45^{11} \ mod \ 233 = 147$, $\beta = 45^{20} \ mod \ 233 = 195$

$\beta^a \ mod \ p = 195^{11} \ mod \ 233 = 169$ and $\alpha = b \ mod \ p = 147^{20} \ mod \ 233 = 169$.

[1] $k = \beta^a \ mod \ p = (bmodp)^a = (g^b \ mod \ p)^a = g^{ba} \ mod \ p = (g^a \ mod \ p)^b = a^b \ mod \ p$

A and B have a private key, $k = 169$.

The security of this method is based on the difficulty of calculating $k = g^{ab}\ mod\ p$ from $g^a\ mod\ p$ and $g^b\ mod\ p$ when p is great.

The function $f(x) = g^x\ mod\ p$ is a one-way function $f(\mathrm{x})$ is easy to compute, but to recover x from $f(\mathrm{x})$, g and p is very difficult (if $y = g^x\ mod\ p$, we say that x is the discrete logarithm of y to base g modulo p).

3.6.2 Cryptographic primitives

Both key transport and key agreement exist in embodiments depend on asymmetric or symmetric cryptography. It should not be a confusion between cryptographic primitives and authentication mechanisms that can be integrated with the key establishment protocol. To make this distinction clear, we take the example of the Diffie-Hellman protocol. Diffie-Hellman is based on asymmetric cryptographic primitives. However, Diffie-Hellman is natively unauthenticated and vulnerable to the man-in-the-middle attack [118], so it must rely on an authentication technique, some of which may be based on symmetric techniques.

We consider only the cryptographic primitive and the cryptographic primitive type, four cases are possible:

- *Key transport based on symmetric cryptographic primitives*: this category includes algorithms in which two peers, already have a shared key derived from each other. This usually happens when a symmetric key has to be refreshed, or when an ephemeral secret like transient session key has to be derived from a long-term one.

- *Key transport based on asymmetric cryptographic primitives*: in this category exist various key establishment protocols from simple one-pass encryption of a secret key using a public key to more complex X.509 [119] keying protocols.

- *Key agreement based on symmetric cryptographic primitives*: a corresponding protocol, the Blom scheme [120]. Dissociate the key agreement protocol

from Diffie-Hellman concept.

- *Key agreement based on asymmetric cryptographic primitives*: with few exceptions, this category consists of the Diffie-Hellman key agreement protocol and its variants.

3.6.3 Authentication method

Authentication of a pairwise key establishment protocol refers to the ability for one or both communicated nodes that undertake it, to bind the established key materiel by the identity of its peer. Even if it is a good thing to possess a protocol for a pairwise key establishment to authenticate both peers to each other, this is not always the case. Generally, just one peer is authenticated to the other.

Some protocols provide authentication natively. For example, this is the case of a one-pass key transport protocol wherein a session key k is sent from a node A to its peer B, encrypted with the public key of B. This protocol provides much more than confidential key delivery: it turns out that a node k namely must be identified as B, since only B should have been able to decipher the message containing k. On the other hand, as mentioned above, the Diffie-Hellman does not provide authentication natively. The Diffie-Hellman public values must be authenticated at communication protocol level.

The key cryptographic primitives underlying authentication method can be classified as symmetric or asymmetric techniques, like those of key establishment protocol. The authentication can be distinguished on the categories that are listed below.

3.6.3.1 Shared secret–based authentication

This is the classic symmetric authentication scheme in which both parties are statically configured with, or otherwise acquire, a common shared secret mapped to their respective identities.

3.6.3.2 Static public key authentication

In this asymmetric authentication scheme, both parties are statically configured with their respective public keys mapped to their respective identities. Demonstrate knowledge of the corresponding private key implicitly ensures ownership of the matching identity.

3.6.3.3 Certificate-based authentication

This is a variant of the preceding category, wherein the mapping of a public key with an identifier is not a static configuration parameter, but is obtained in the form of a signed certificate. The certificate-based authentication requires that a third party, called the certificate authority, be approved by both authenticating peers.

3.6.3.4 Cryptographically generated identifiers

This family of asymmetric techniques changes the implicit assumption that any type of identifier can be authenticated, provided it is well linked to a public key. These techniques presuppose that authenticated the identifier of a node is obtained from the public key of the node, for example, as a hash of the public key. Mechanisms are then defined in order to construct protocol stack identifiers (typically, IPv6 addresses) from these cryptographically generated identifiers.

3.6.3.5 Identity-based authentication

This latest series of technical asymmetrical bases on the paradigm Identity Based Cryptography in which, in contrast to the previous category, the public key of a node is derived from its identity (whatever the format of this identity). As in all asymmetric techniques, a node proves its identity by providing proof of knowledge of the corresponding private key.

3.6.4 Symmetric vs. Asymmetric

Each of these two forms of cryptography has its own advantages and disadvantages. In the case of LoWPAN networks, which are constrained networks, symmetric cryptography is often favored over the public-key cryptography for the following two reasons:

- The data processing speed is higher in the case of a symmetric cipher, which leads to an energy consumption and computation time much less important.
- The size of the keys and packets encrypted or signed is much lower for the same level of safety in the case of symmetric cryptography.

3.7 IDS : Intrusion Detection System

Unlike cryptography, the system has the ability to detect with high accuracy internal attacks. This mechanism is used to detect abnormal or suspicious activities on the analyzed target and trigger an alarm when malicious behavior occurs. The cryptography mechanisms are not effective when protecting against insider threats, also it cannot defend against some external threats like DoS attack from the Internet to the LoWPAN network.

3.7.1 The main components of an IDS agent

IDS agent is installed in the application layer, it consists of three components (or modules). These components are defined as follows:

- *Data Collection*: this module is responsible for packet capture in the radio range of the node IDS.
- *Intrusion Detection*: IDS agent analyzes the captured packets in a policy based on detection. Among these policies, there's the signature-based detection of

attacking and anomaly detection. These techniques will be detailed in the next paragraphs.

- *Prevention*: intrusion prevention is a set of tasks designed to anticipate and stop attacks. These tasks can be defined such as sending an alarm by the IDS to the base station, the latter subsequently ejects the suspect node of the network and apply the update key.

3.7.2 IDS in a LoWPAN

The IDS solutions developed for ad hoc networks cannot be applied directly to LoWPAN networks, and this is due to the difference of these two types of networks [121]:

- In ad hoc networks, each node is typically handled by a human user. Unlike LoWPAN where all nodes are independent, these sensors send their collected data at the base station. The latter is usually controlled by a human user.
- Energy resources are more limited in the LoWPAN nodes compared to ad hoc nodes.
- The task of the LoWPAN network is very specific, for example the measurement of the temperature in an agricultural field. Therefore, the hardware modules and communication protocols must depend on the intended application.
- The density of nodes in LoWPAN networks is higher than in the ad hoc networks.

Thus, it is necessary to introduce a mechanism for detecting the own LoWPAN network intrusion.

3.7.3 Intrusion detection policies

The political intrusion detection in LoWPAN networks can be classified into two main techniques, signature-based detection and anomaly detection.

3.7.3.1 Signature-based detection

This approach is based on comparing the observed node behavior with a set of attack signatures stored in its memory. If a match is found, the analyzed node is defined as an attacker. This technique is precisely known for the detection of attacks. The disadvantage of this technique is the inability to identify unknown attacks. The reliability of this technique is based on the continuous updating of the signatures, so this leads to a memory overload.

3.7.3.2 Anomaly detection

This approach is based primarily on modeling the normal behavior of a node and then identify anything that deviates from this model as an anomaly. This technique consists of two categories: detection based on a binary classification and specification-based detection.

- *Detection based on a binary classification*: this feature uses a supervised learning algorithm to model the normal behavior. The main advantage of this technique is the ability to detect unknown attacks, but it causes a high computational cost, which leads to a decrease in the lifetime of the node. The goal of these learning algorithms is to classify the data as normal or abnormal with a low false positive rate. Therefore, the use of this learning technique in the LoWPAN must consider energy constraints of the LoWPAN nodes.

- *Specification-based detection*: this category models the normal behavior by using a set of rules. The advantage of this technique is the ability to detect unknown attacks with low computational cost. However, the reliability of

this approach relies on the continuous updating of the rules over time. Several researchers have defined rules to detect certain types of attacks. Indeed, in [122] the authors propose a set of rules to detect attacks like: Hello flood, Blackhole, Selective forwarding, Jamming, Wormhole, and Denial of Service (DoS). A continuous update of these rules should be applied for the effective detection of these attacks.

3.7.4 IDS implementation requirements

Much research in the application of the solution of IDSs in ad hoc networks have been done compared to LoWPAN networks, due to limited resources of LoWPAN nodes in terms of computing capabilities and communication. The design of an IDS solution for such networks should consider the following limitations [122]:

- *Waste of energy*: most of the energy consumed in a LoWPAN is mainly due to the communication interface, not the calculation process. Therefore, IDSs must preserve their transmission power and minimizing the data exchange between nodes.
- *Distributed IDS*: in LoWPANs, the base station cannot handle a large number of audit data (intrusion detection) from the network to detect any intrusion. In addition, the nodes cannot transmit a large number of packets because energy resources are not used optimally. This is due to a significant packet transmission to the base station. In this case, a distributed detection based on the cooperation of IDS agents is a desirable solution.
- *No node is trustworthy*: each IDS agent monitors its neighbors, based on the fact that even the IDS node can be malicious.
- *Real time*: to minimize the impact of a possible attack in critical applications, it is important that an IDS works in real time.
- *Support adding new nodes*: in practice, it is likely that new nodes can join the network after deployment thereof. The IDS must support this transaction

and distinguish normal node from malicious node.

- *Accuracy*: the accuracy of an IDS in LoWPAN is another major problem. It can be defined as the ability of an IDS to determine whether the node in question is malicious or not.
- *Availability*: an IDS must run continuously and be transparent to users.

3.7.5 Evaluation metrics

To evaluate the effectiveness of any proposed IDS model, there is a set of metrics to be adopted to quantify the level of security and the best use of resources such as energy and storage. These performance indicators will enable a network administrator to choose the best intrusion system [123] and the optimization of the location of the agents in the IDS. Accordingly, the following metrics are considered important characteristics for effective design of IDSs in LoWPAN:

- *Detection rates:* represents the percentage of detecting attacks within the total number of attacks.
- *False positives rate (false alarms)*: This is the ratio between the number of classified as an anomaly on the total number of normal connections.
- *False negative rate*: it is the opposite of the detection rate; this metric is defined as the ratio of false detections of attacks on the total number of attacks.

3.7.6 IDS agents' location

An important criterion for achieving the IDS mechanisms in the LoWPAN is the location of its agents in this type of network. Many researchers have worked on this problem [124]–[126].

The network-based approach puts the IDS agent at the base station to receive and analyze data from monitored nodes. In this way, we benefit from the base station strong resources and its global vision of the entire network, which helps detect cooperation attacks. However, the disadvantage of this architecture is that

it creates a lot of communication overhead and is not performing at detecting local attacks.

Otherwise, the host-based approach puts the IDS agents at each node, where each one of them has to monitor data, analyze it and decide for itself. The benefit of this approach is the reduction of monitored traffic. However, it puts more computational work on the node, which shortens its life by consuming its resources. One advantage of this approach is the ability to detect local attacks, but it lacks the global vision, which does not detect cooperation attacks.

There is another approach, the hierarchical approach [126]. It consists of combining the two previous solutions in the network. It places the IDS agents on three levels. The first is the level of the cluster members, which are used to control the behavior of their neighbors and collect audit data. These nodes have the ability to analyze their own data to identify malicious neighbors to isolate them. The second is the level of cluster-heads, which are used as coordinators to consolidate audit data from their cluster nodes, analyze and make decisions to identify intrusions. The highest level is the base station, which collects data to monitor its cluster-heads and detects attacks across multiple clusters.

The main advantages of this architecture are the ability to detect distributed attacks and ensure scalability. Audit data collected from different points of view of the network also allows robust and fault-tolerant architecture [126]. The clustering architecture in LoWPAN is similar to the 6LoWPAN graph topology (RPL DODAG) where the border router 6LBR is placed on the side of Internet and acts as a base station. The border router is typically a wired device connected to the Internet so that it can be considered unlimited resource.

The DODAG roots will act as cluster heads for controlling operation of sensor nodes. Algorithms for attacks supervision in each DODAG will be slightly different because each uses a different objective function and follow DODAG varied routing rule. It is not in the clustering topology where cluster-heads implement the same algorithm. However, it does not affect cooperation between DODAG roots because the border router always has a global vision.

3.8 Analytical study

IEEE 802.15.4 and IPv6 networks have their own security mechanisms, we must therefore study them in order to consider possible solutions adopted for the 6LoWPAN network. The solution must be found to communicate via the Internet. We can ensure the end-to-end security only in the level of layer 3, the network layer. However, the provision of end-to-end security of the data is not enough, protecting the lower layers will ensure the protection of internal communication channels, especially being vulnerable to several attacks being wireless, as well as increases the protection and privacy of data.

We will study the security mechanisms each of 802.15.4, which represents the main criterion for layer 2, data link layer, and the IPv6 protocol, which is the main protocol for layer 3.

3.8.1 IEEE 802.15.4 security mechanisms

IEEE 802.15.4 networks has two modes: secured mode or unsecured mode. Unsecured mode especially in devices that are not support mechanisms of security and have a negative impact on its capacity, but the device remains in this situation at all the possibilities of risks, but it can here resort to security solutions of the upper classes.

Since we are studying the security, we will focus on the study of the secured mode, a mode that adopts the AES (Advanced Encryption Standard) [72] algorithm for symmetric encryption, in addition to other services: access control, frame integrity, sequential freshness. Security keys are provided by the upper classes, but the establishment and management systems are not defined by 802.15.4 standard due to the different and multiple applications that use it, the variations in needs and the environment where it operates is not determined. As for access control, it allows the selection of the device authorized to communicate with it. Frame integrity used to protect the data from tampering, as well as to ensure the reliability of the sender is the owner of the key. Finally, sequential freshness is used to ensure the sequential order of the frames and ensure they do not recur in the future.

IEEE 802.15.4 requires the support of cryptographic mechanisms strong enough for each node, a requirement that is completely filled by most IEEE 802.15.4 chips available today. The encryption mechanism is selected based on modern AES that uses the CBC-MAC (CCM) counter mode [72], which provides not only encryption but also an integrity check mechanism.

By combining encryption with authentication, some of authenticated information can be sent in the clear. AES-CCM therefore encrypts a message m and authenticates that, with additional authenticated data a using a secret key K and a nonce N. A parameter L controls the number of bytes used to count the blocks in the AES message; m should be less than 2^{8L} bytes. For IEEE 802.15.4 packet, the smallest value of L = 2 is sufficient. The nonce N is of length 15 - L, i.e. 13 bytes for IEEE 802.15.4. The nonce is not a secret, but must be used more than once: If an attacker has access to two messages encrypted with the same K and N, the security properties of AES-CCM are lost. The result of AES-CCM is an encrypted message of the same length as m and an authentication value of length M bytes, where M is a parameter that can be any value, between 4 and 16, but is limited in scope and a value of 0 (no authentication), 4, 8 or 16 bytes in the IEEE 802.15.4 standard. The authentication value cannot be created correctly when K is known, it can be controlled by the receiver to ensure that m has not been altered by an unauthorized party.

AES-CCM is a very effective and very safe algorithm, as long as the same nonce N never occurs twice with the same key K. IEEE 802.15.4 built the 13 bytes nonce from the eight bytes full address of the device originating the encrypted frame, a four bytes frame counter, and a one byte field occupied by the IEEE 802.15.4 security level.

So how do IEEE 802.15.4 ensure that a nonce is never used twice? The source address and the security level surely repeat. Thus, the security of the entire scheme rests on the four bytes frame counter. It lets sending up to 2^{32} encrypted frames from a source before the key that was used for these frames is exhausted, assuming that the node has a stable storage, which saves the frame counter current reliably even across node resets. Note that if this knowledge is lost, the key K must be

changed to remain secure.

3.8.2 IPv6 security mechanisms

Even with the best data link layer security mechanisms in the LoWPAN, data are not protected once it leaves the link. This makes data vulnerable to any point that is responsible for forwarding it to the network layer, or a link that has less security. Even worse, an attack on the network layer may be able to divert data onto a path that contains additional forwarding nodes controlled by the attacker.

End-to-end security that protects the conversation along the entire path between two communicating nodes is an important component of any robust security system, so that this requirement has become a feature in the development of IPv6. Security features arising have been ported to IPv4 and are quite independent of the IP version that they are known as IPsec [127].

IPsec has two main components: the packet formats and related specifications that define mechanisms of confidentiality and integrity of the data, and a key management system Internet Key Exchange (IKE [128], updated by IKEv2 [129]). The relatively complex set of IKE protocols is generally considered a poor fit for the requirements of LoWPANs.

IPsec defines two formats of data packets protected by encryption: the IP Authentication Header (AH) [130], which protects the integrity and authentication only, and the IP Encapsulating Security Payload (ESP) [131], which combines this function with the protection of confidentiality through encryption.

The Security Parameters Index (SPI) identifies specific security settings, including the keying material, used for this direction of the conversation (security association). For unicast packets, the SPI is an identifier of local importance for the receiver, i.e. it is affected by the receiver in a way that facilitates its local processing of the incoming ESP packets. The sequence number is a 32-bit unsigned increasing by one for each packet sent on the security association; it can also be the lower 32 bits of a sequence number of 64 bits stored in the security association. The payload data and the trailer comprises stuffing the buffer length and another header

field, are part of the package that is encrypted.

The end-to-end principle argues that many functions can be implemented properly as a base from end to end, including ensuring the reliable delivery of data and the use of cryptography to ensure the integrity and confidentiality of a message [132]. Adding a function to improve the reliability of a particular route can provide some optimization, but cannot guarantee end-to-end reliable delivery. Similarly, the security objectives that can be met only by securing the conversation between two end nodes are better met by carrying cryptography at the network layer or higher; it may even be the security objectives that require the protection of the data itself instead of the communication channel. However, this does not mean that all security objectives can be met from end-to-end. In particular, achieving robust availability often requires protection subnet against attacks, especially for wireless networks. Adding a first line of defense in the link layer can also increase the robustness against attacks on the confidentiality and integrity.

3.9 Discussion & conclusion

One of the most important aspects to consider when creating a 6LoWPAN network is setting the security mechanisms and maintain it. 6LoWPAN networks are inherently open to the attackers whose aim to introduce false information affecting the cost-effectiveness and quality of the network, or to tamper the functioning of the full network as a whole or a part of it as Denial of Service attacks. Attacks can be done via a malicious node, a powerful machine placed approximately to the LoWPAN, or remotely through the Internet. The specific features of 6LoWPAN networks (limited energy, low-power computing, wireless communication, etc.) expose its nodes to many threats. While some of these threats can be found in all ad hoc networks, others are specific to this type of network and is designed specifically to address the limited energy of sensors. Unfortunately, current security systems used in today's networks are not suitable, even if they are more complicated or they are insufficient. Any proposal to resolve the terms of the security of 6loWPAN network must take into account two factors; the need to use limited resources

and the need for minimal consumption of energy.

6LoWPAN threats can be divided into two categories. One aims to violate the network confidentiality, authentication, and integrity, which can only be protected by a cryptographic solution, and the other aims to break the network performance, which may be protected using an intrusion detection system. The purpose of security is to provide a system of encryption that protects network data and a monitoring system that will attempt to detect the abnormal malicious behavior in the operation of the network and prevent it from harming the network performance.

In most current security mechanisms, cryptography is probably the most used technique. Data encryption prevents eavesdropping data transmitted over a wireless network and ensure data confidentiality. The current research focus on finding so-called lightweight cryptography solutions. These solutions consist in adapting traditional cryptographic algorithms for sensor networks, or finding new ones just as effective in terms of security, execution time and energy consumption. These solutions are of two types of cryptography: symmetric cryptography and asymmetric cryptography, commonly called public key cryptography. Each of these two forms has its own advantages and disadvantages. In the case of LoWPAN networks, which are low power networks, symmetric cryptography is often favored over the public key cryptography for the following reasons: The data processing speed is higher in the case of a symmetric cipher, which leads to an energy consumption and computation time much less important. In addition, the size of the keys and packets encrypted or signed is much lower for the same level of safety as the asymmetric cryptography.

However, the cryptography mechanisms are not effective when protecting against insider threats, also it cannot defend against some external threats like Denial of Service attacks from outside the network. That is why there are the Intrusion Detection Systems (IDS). Unlike cryptography, the IDS has the ability to detect with high accuracy internal attacks. This mechanism is used to detect abnormal or suspicious activities on the analyzed target and trigger an alarm when malicious behavior occurs.

The design of an IDS solution for 6LoWPAN networks should preserve trans-

mission power and minimizing the data exchange between nodes, to minimize the impact of a possible attack in critical applications, it is important that an IDS works in real time and each IDS agent monitors its neighbors, based on the fact that even the IDS node can be malicious. In addition, a distributed IDS based on the cooperation of IDS agents is a desirable solution in order to minimize to overhead in the network.

In general, the main challenge in the designing of a security system for the 6LoWPAN network is to select optimal techniques that must adapt with 6LoWPAN resource constraints. Such a system can be built with many options that exploit network architectures and features. A normal network performance can be guaranteed only if the network is in its optimized topology; each node works with its reasonable capacity. The issue of energy because the addition of a new system to the network can be solved using the topology and protocols used by the 6LoWPAN, such as parent-child hierarchical architecture built by RPL protocol, to minimize the computation workload and the communication overhead over the network, also by the choice of lightweight techniques such as symmetric cryptography and distributed intrusion detection system. 6LoWPAN security system that we propose works based on these two cited concepts, i.e. using the system architecture and lightweight techniques. It was designed with two lines of defense, the first line is provided by cryptographic mechanisms to prevent and eliminate outsiders to join the network. For our e-healthcare system, it is considered to solve the confidentiality, privacy, authentication, and integrity. In addition, the second line of defense is used to solve the other security requirements does are not assured by cryptography, like availability, robustness and resiliency, so we built the IDS to monitor and detect malicious sources from the early phase to eliminate further damage of the attacks.

We tried to follow the conclusions of the analyzes we did in this chapter to avoid the shortcomings of existing solutions. Thus, we propose one system that simultaneously provides the security of internal and external 6LoWPAN communications, where most of the existing solutions only focuses on one side. In addition, we propose an intrusion detection system concept that protects the functionality

and availability of 6LoWPAN networks. Although our solution is designed for e-healthcare applications, it can be adapted to other areas.

According to our study in this chapter, we concluded that symmetric cryptography is the most suitable for 6LoWPAN networks compared to asymmetric cryptography, since it does not consume energy, fast and the keys size is small. However, the major issue with this kind of cryptography is key establishment, especially as 6LoWPAN networks will need to communicate through the Internet with other strange devices; whose do not share pre-established information. We propose a system of key management for the symmetric cryptography that provides a complete and energy-efficient solution.

Thus, as regards the intrusion detection system, we established a set of requirements that IDS must meet, such as preserving transmission power, minimizing the data exchange between nodes, minimizing the impact of a possible attack in critical applications, working in real time, monitoring neighbors, and be in distributed way basing on the cooperation of IDS agents. We designed a system that meets these requirements, while providing a high level of intrusion detection and consumes less energy.

We have summarized the main requirements that we must deal with it in order to design a security system complies with 6LoWPAN networks for e-healthcare applications in the Internet of Things context. The details of our solution will be treated apart in the following chapters. The first one is the key establishment system and the second one is the intrusion detection system.

Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet.

Gary Kovacs

4

Key Establishment System

6LoWPAN combines two different networks: 802.15.4 and IPv6. There are key establishment solutions suitable for each of the two types, but the solutions that deal with LoWPAN networks treated as an isolated network and manages only hop-by-hop communications. Regarding communications through the Internet in the end-to-end way, there is adapted solutions from existing protocols for low power devices, but they only treat the end-to-end communications between two separated devices and does not deal with inter-LoWPAN communications. Since 6LoWPAN network has the low-power as main feature, the use of many protocols at once will consume more energy and occupies more storage and memory space.

4.1 Related works

The research for energy efficiency solutions was conducted to accommodate the limited resources of LoWPAN. For this, the design of an institution key cryptography suitable for this kind of network system was a necessity and a huge challenge. However, the proposed solutions have been designed to be adapted to existing topologies of LoWPAN networks being isolated networks where nodes exchange messages with each other through hop-by-hop communication. Their connection to the Internet passes through the base station, and therefore it does not have direct communication with external devices on the Internet. Above all, these devices rely on communications at the data link layer, which is offered through the IEEE 802.15.4 standard battery light communication and effective management of bandwidth.

With the addition of the 6LoWPAN layer, the sensor nodes support communication with other IP devices outside the LoWPAN network where they are located, like any IP machine communications, through end-to-end way. Hence, the need for security mechanisms to secure end-to-end communications with other IP hosts.

The adaptation of existing end-to-end security protocols, like IPsec, to LoWPAN networks will pose several constraints. These protocols were designed for unconstrained machines and their adaptation will require reshaping in terms of state machine complexity, data structures, and cryptographic primitives. Consequently, recent proposals describe lightweight versions of existing protocols to implement them in devices with resource constraints.

Since 6LoWPAN technology is new, there is not a lot of key establishment solutions in the literature specifically designed for such networks. For this, we examine in this section the approaches proposed for the establishment of light keys to LoWPAN nodes in general. The cited systems are divided into two groups, the first is for solutions for conventional LoWPAN networks, and the second for approaches that aim to adapt the Internet security protocols designed for the IP based LoWPAN nodes. We relied on the following documents [133]-[137] to achieve the

analysis.

4.1.1 Key establishment schemes in simple LoWPANs

Several key establishment schemes have been proposed for traditional LoWPAN networks such as WSNs, in order to cope with resource constraints of the nodes of these networks. Most of the proposed approaches are based on symmetric cryptography because of their low resource consumption. These solutions are considered most effective for the sensor nodes. The most relevant research is described in the following.

The best-known is the pre-distribution solution that aim to put the same master key in all nodes. Any pair of nodes can then use this global secret key for key establishment and exchange a secret key pairs. However, this solution is very vulnerable to node compromise because a successful attack on a node will allow recovery of the secret master key, which means that the entire security system network is interrupted.

Another system of pre-distribution key is to hold each node with N-1 secret key pairs, each pair being shared between the node and one of the other N-1 nodes (N being the total number of nodes). However, this system is not viable for nodes with very limited storage capacity, because N could be great. Eshenauer & Gligor proposed a pre-random key distribution: random key sets are distributed to each sensor and, after deployment, a pair of nodes having at least a common key to be used as a secret key pairs. Chan & al. in [138] proposed a q-composite random pre-distribution key system improving network resiliency compared to the Eschenauer-Gligor scheme. The difference is that q common keys - instead of one - are needed to establish secure communications between a pair of nodes. The shared secret key is the hash of the q common keys.

Liu & al. proposed in [139] a system of pre-distribution key based on the knowledge of the deployment, to improve the probability of key sharing. The keys are allocated based on the geographical position of the nodes. A similar approach is also developed in [140]. These solutions are not practical in networks with a topology

deployed randomly. In [141], they propose a polynomial based pre-distribution key scheme, a polynomial share is distributed to each node where any two nodes are able to establish a pairwise key by using it.

Perrig & al. proposed in [142] SPINS, a key management protocol that relies on a trusted base station to distribute keys. Two nodes use the base station as a trusted third party to create their private key pairs. SPINS has two parts: SNEP (Secure Network Encryption Protocol) that secures communications between a node and the base station or between two nodes, and μTESLA (μTime Efficient Streaming Loss-tolerant Authentication) that authenticates packets from the base station.

However, proposed systems based on symmetric keys are only applicable to local nodes, which are considered to belong to LoWPAN networks, themselves connected to the Internet via dedicated gateways. These systems are based on pre-shared key between the different nodes of the same network. Given the scenarios of the Internet of Things, a sensor node is considered a part of the Internet, able to establish end-to-end communications with external entities without requiring initial knowledge of these external entities, any prior authentication context or any pre-shared keys. In terms of security, these schemes are based on the data link layer security and are particularly vulnerable to node compromise. Scalability and complex key management are also important issues that are considering a network of large scale nodes that needs to generate a large number of shared keys and then install them in the nodes before deployment.

To eliminate the complexity of key management and increase the level of security in the LoWPAN networks, many researchers have studied the application of asymmetric cryptography in LoWPAN networks in order to provide the best combination of security services, computation overhead, and memory requirements. The security services (such as non-repudiation) and the level of protection (e.g. resilience to node compromise), it offers more advanced than those offered by the symmetric cryptography. Lopez [143] highlights the limitations of the use of symmetric cryptography in sensor networks and promoting based on public key cryptography to enhance security of the entire system solutions, while setting guard

against complex calculations. The author emphasizes the important role that Elliptic Curve Cryptography (ECC) [144] can play in overcoming the computational complexity of public key algorithms.

ECC has been the first choice among the various public cryptographic algorithms because of its low power consumption, fast processing times, compact signatures, and small key. For example, a 160-bit ECC key size ensures a level equivalent to an RSA 1024-bit key protection with reduced energy consumption by half [145]. The authors of [146] setting light work presents algorithms of public key cryptography based on elliptic curves and argue that the use of the property based ECC key solution is the best compromise between consumption and the energy level of security.

In [147], [148], they focus on taking RSA public key cryptosystem to make it more suitable for resource constrained devices using a small RSA public exponent (e) and a short key size. For example, Watro & al. in [148] develop TinyPK system that allows the implementation of PKI (Public Key Infrastructure) in LoWPAN networks. The concept requires the use of smaller RSA parameters (key size exponent) and the use of public key operations only in the sensor device. This comes, however, at the cost of a lower level of security [149]. Huang & al. [150] and Kotzanikolaou & al. [151] proposed hybrid protocols that combine standard Elliptic Curve Diffie-Hellman (ECDH) key agreement and implicit certificates with symmetric techniques in an effort to reduce the elliptic curve random point scalar multiplications on the expensive side of the sensor. The cost per node for key establishment is effective due to the combination of symmetric encryption in the randomization process and use of Schnorr signatures.

This approach reduces the high cost of public key operations by replacing the asymmetric key operations with those based on symmetric keys and joins the advantages of both approaches. However, communications with an external party became less possible, since both peers must share a symmetric key.

To make public key cryptography practical in LoWPAN networks, [152], [153] have proposed hardware solutions that extend computing capabilities of a standard node with low power hardware modules. The results show that these additional

hardware implementations help provide security services with lower energy consumption and low cost. However, it could be a difficult task given the small and inexpensive detection devices design.

With the wide deployment of WSN applications, another model of sensor networks, called Heterogeneous WSN (HSN) has emerged in recent years. Unlike the homogeneous sensor network, in heterogeneous networks various sensors with different capabilities, detection for different applications coexist in the same controlled environment. Accordingly, Mache & al. developed in [154] a framework for establishing key resource restricted hybrid sensor networks that exploits heterogeneous deployment of sensor node, based on a combination of symmetric and asymmetric operations. The idea is to use on the first part of the path from sensor to sink, a less expensive symmetric cryptography until a resource-rich gateway is reached, and then, on the second part of the path, to use more expensive publik key cryptography.

Riaz & al. proposed in [155] three settlement systems of keys: SACK based on symmetric key cryptography, SACK-P based on the asymmetric key cryptography and SACK-H that is based on a hybrid approach of using asymmetric cryptography for cluster communication wide and symmetric cryptography to network wide communication. The authors then make a comparison between the three proposed schemes and show that SACK is light on resource consumption, but has a low level of security, as a compromise node makes the entire network vulnerable. However, SACK-P is heavy on resource consumption, but provides the level of the highest security with maximum knot strength compromise. The SACK-H hybrid system is between the other two and this consumption of resources in the medium with a medium-security.

However, security is ensured in these schemes on a hop-by-hop. Confidentiality and availability are compromised because the entity of intermediate translation on the border between "symmetric" and "asymmetric" areas potentially introduces both a security and a single point of failure.

4.1.2 Key establishment solutions in IP enabled LoWPANs

The solutions discussed above for key establishment in the LoWPAN networks are not designed a secure end-to-end communication between the LoWPAN node and the remote hosts. Instead, they discuss the security of communications within the network. Recently, with the advent of the integration of LoWPAN networks to the Internet (6loWPAN), the need for an end-to-end security protocol between nodes and detection of Internet legacy was recognized. To enable functional implementations of Internet security protocols like TLS and IPsec in a constrained environment, settlement schemes have been proposed lightweight keys. They rely on the use of modified protocols corresponding strikes implementations of TLS (Transport Layer Security) [158], IKE (Internet Key Exchange) [128] and HIP BEX (Host Identity Protocol Base Exchange) [157].

When a TLS connection is required between a client and a server, a first phase called TLS Handshake [158] is to negotiate security algorithms to authenticate at least one station to another and establish a shared secret between two peers. The TLS Handshake supports two different methods of key exchange: a key transport method based on asymmetric cryptography and RSA tuning method of Diffie-Hellman. Note first that the pre-shared key to use the key exchange in TLS-PSK (TLS Pre-Shared Key) [159] cannot be practiced between LoWPAN nodes because of the lack of context initial authentication between them.

As explained above, the use of ECC has been generally regarded as the most appropriate among other public key cryptography into existing networks of sensors choice. Consequently, there are two different implementations of lightweight TLS on the constrained-devices based on ECC for key exchange while maintaining the same message exchanges. Sizzle [160] was the first security protocol that proposed the use of TLS in the LoWPAN to implement a stack of HTTPS. Sizzle is based on translating gateways that correspond to the nodes of local sensors (non-IP) hosting Internet IP addresses, allowing them to exchange data directly with their remote IP peers. During the TLS negotiation, the Elliptic Curve Diffie-Hellman (ECDH) key agreement [161] and the Elliptic Curve Digital Signature Algorithm

(ECDSA) [162] respectively replace the Diffie-Hellman key exchange and DSA (Digital Signature Algorithm). Using these protocols based on ECC, performance evaluations have shown that the implementation of HTTPS Web servers on the LoWPAN nodes can be bearable for rare connections. SSNAIL [163] was developed as second lightweight TLS implementation for LoWPAN networks based on IP relying on the same cryptographic primitives as Sizzle for key exchange while eliminating the use of the bridge. Authors measure the implementation of a few handful based ECC takes about one second while it takes 8.5 seconds for an RSA database.

The purpose of IKE is to establish a secure channel between two parties and allow them to authenticate each other. IKE provides a protocol to establish security associations (SA) required for IP datagrams using IPsec. In 2011, a first tableting implement IPsec for 6LoWPAN networks has been proposed [164], based on pre-shared key for exchanging keys. Authors acknowledge that the use of pre-shared keys is not a possible solution for sensor nodes that must be able to communicate with external hosts without the need for authentication before contexts. They are currently studying the feasibility of Internet Key Exchange for IPsec on 6LoWPAN.

Regardless of integrating LoWPAN to the Internet, two recent variants of IKE have been proposed for the purpose of energy efficiency. V. Nagalakshmi in [165] modifies the IKE eliminating pseudorandom functions of production, eliminating the repetitive use during the key exchange. The transmitter sends a hash of its private key and its private Diffie-Hellman value instead of sending nuncios. The proposed work led to the business, but the energy cost of generating pseudo random function (for a total symmetric encryption) can be neglected compared to the importance of the cost of asymmetric cryptographic operations necessary further in the protocol exchange. In 2012, ECC-based IKE protocol [166] was designed for Internet applications. It aims to reduce the burden of the exchange IKE base using ECDH key exchange to establish the shared key and the use of public key certificate based on ECC for authentication of communicating entities.

HIP BEX aims to generate key material for later use by IPsec to establish secure

communication from start to finish between the two entities. However, unlike IKE, no certificate is required for authentication HIP BEX because self-certification identifiers are used. The concept of an "identifier self-certification" can be explained as follows: it is an identifier that only the rightful owner can use, without the need for external evidence from a third trust (certificate) to claim it property. To achieve this functionality, the identifier of the self-certification is generally constructed as a Cryptographically Generated Identifier (CGA) [167]. This must be linked to a unique public key whose its private counterpart is known as the rightful owner, hence its denomination. Thus, evidence of a certain CGA property reverts to prove ownership of the public/private key pair bound, hence the possibility of using the corresponding private key. In HIP, the CGA used to identify a node is the number of the Host Identity Tag (HIT), which is a 128-bit hash of the public key. The objective of the base HIP Exchange (BEX) is to perform a key agreement between two authenticated HIP peers.

Arose from the observation of the cost of supercomputing HIP Base Exchange, two modifications have been proposed to make the protocol used by constrained. HIP Diet Exchange (DEX) [168] proposed a long-term node use Elliptic Curve Diffie-Hellman (ECDH) public value as its host identifier. DEX will adjust the key exchange, and Lightweight HIP (LHIP) [169], a much more radical approach, which maintains the same message syntax as in HIP BEX for compatibility reasons but do not use any security HIP BEX mechanisms. No Diffie-Hellman key is calculated, no operation is performed and no RSA secure IPsec tunnel is established after the exchange. Instead, the channels are used for successive hashing cryptographically bind messages to each other, representing a minimum level of security.

LHIP trades security for energy efficiency drastically. Its security level is very low: only HIP control messages are protected by hashes integrity. This weak security property assurances only that an ongoing session has not been hijacked (temporal separation property), but does not provide strong node authentication. In addition, HIP data messages are not protected as no mechanism for key exchange is provided.

Most of the modified TLS, IKE and HIP BEX variants are based on the use of

ECC algorithms. In [170], a comparative performance analysis was conducted between RSA-based and ECC-based TLS handshakes on a standard PC. The results showed that the use of ECC reduced by 37 percent the energy consumption of the process of establishing TLS key comparing to RSA. Liu & al. in [171] implemented ECC in TinyOS for many platforms, including MICAz and TelosB. They assessed the (160-bit key) point multiplications costs necessary to make the exchange ECDH and ECDSA signatures. The results showed that the energy cost of ECDH-ECDSA key agreement protocol is about 236 mJ to 72 mJ for MICAz and TelosB. A DH-RSA key agreement protocol uses about 190 mJ on a TelosB. Thus, the energy consumed by the use of ECC is reduced by 62 percent.

However, these energy costs measured of ECC are still significant, being of the order of magnitude of milli-joules. In practice, these energy costs would be hindering for highly resource-constrained nodes. Authors in [172] investigate the practical use of ECC devices constraints in LoWPAN networks and perform a cost comparison between the two regimes setting ECDH-ECDSA and Kerberos (a server-assisted key distribution protocol assisted based on symmetric cryptography). They conclude that Kerberos is 95 times cheaper than ECDH-ECDSA on a platform MICAz detection.

4.1.3 Discussion

Even if 6LoWPAN networks has, approximately, the same features of other low power wireless networks, but the difference of its ability to connect directly to the Internet makes it an independent network that has its own requirements. As presented above, neither the security schemes proposed for simple LoWPAN networks or nor proposed for IP-based ones are suitable, because the first lacks the end-to-end security, and the second consumes much energy.

As the Internet of Things is new and still emerging, there is a few solutions for key establishment in such networks, but as seen, all of them treat only the end-to-end issue side. However, the 6LoWPAN has two communications types, an internal communication between the LoWPAN nodes, and an external one through

the Internet with IP hosts, which may be a normal machine, or another 6LoWPAN node. We can combine more than a solution with different mechanisms in the same network, one for internal communications, and other for external ones, but for optimization purposes, it is much better to adopt one solution that is valid for both of them.

Much work has been done to prove the practice of asymmetric key cryptography for LoWPANs but no particular architecture key establishment for 6LoWPAN has been proposed yet. Many key establishment solutions have been proposed with systems of symmetric keys, but end-to-end communications cannot be secured by these schemes. To our knowledge, no work has a complete solution for key establishment framework for 6LoWPAN networks, which provides flexibility to integrate internal and external communications designed to the according to the Internet of e-healthcare things applications requirements.

We conclude from what we studied above and in previous sections, any proposed solution for key establishment in 6LoWPAN networks should:

- provide security for internal and external (end-to-end) communications.
- be appropriate for an heterogeneous network.
- be based on symmetric cryptography as it does not consume energy.
- not be based on pre-shared keys as any 6LoWPAN node must be able to communicate with an external device that it does not share with it any information.
- avoid a whole network group based keys.
- provide session keys.
- support mobility.

4.2 Proposed solution

In our proposed key establishment scheme solution for 6LoWPAN networks, we tried to respect the requirements that we conclude from the analytical study of the 6LoWPAN features, its security requirement [173] and different proposed solutions, all in respect with application domain, which is the e-healthcare in the Internet of Things context [174].

We chose to deal with symmetric cryptography as it is an energy-efficient solution [175] as we conclude from the previous studies. To deal with the issue of keys establishment, we designed a solution where we generates the key on the node without any pre-shared key, avoiding the risk of keys eavesdropping by attackers.

In the studied system, we have three types of e-healthcare devices: WBAN, WPAN, and the Remote Server in the Medical Center Unit. We obtain approximately two types of communication, between:

- a 6LoWPAN node (WBAN or WPAN) and a remote server.
- two 6LoWPAN nodes (WPAN) in the same 6LoWPAN network.

In addition of two other types of communication imposed by the Internet of Things requirements:

- a 6LoWPAN node and an IP-host.
- a 6LoWPAN node and other 6LoWPAN node of another network (through the Internet).

We designed our scheme to provide a solution for key establishment in 6LoWPAN networks to ensure its security, taking into account the performance requirements as energy optimization, scalability, flexibility, mobility and connectivity. Our solution provides three types of security keys: a pairwise key between the MCU and each node on the 6LoWPAN network, a group key shared between a parent node and its children nodes, and an end-to-end session key between a 6LoWPAN node and other IP device on the Internet.

As our solution is based on symmetric cryptography, we chose to use AES (Advanced Encryption Standard) algorithm since it is the most used in LoWPAN networks and has been ranked the best symmetric algorithm [176].

4.2.1 Assumptions

We consider a 6LoWPAN network consisting of a set of nodes, WBAN devices implemented on the monitored person body, WPAN devices implemented in its environment, a gateway device that relies the WBAN and the border router 6LBR; the bridge between the nodes and the Internet, and a remote server; the Medical Server Unit (MCU). According to the RPL protocol, WPAN nodes form the topology parent-son tree according to the scheme designed by the DODAG (section 2.8.2 p. 69), the information flow destination within the 6LoWPAN network is either upward or downward, from or to the 6LBR.

We assume that the immediate neighboring nodes of any device will not be known in advance. Some nodes serves as a router (6LR) between the other nodes and the 6LBR. Each node has a unique and secret identifier *sID*. The MCU installed remotely plays the role of the network monitoring. This MCU is equipped with a database implemented by the 6LoWPAN's nodes information. The necessary information we will need in this database are the nodes physical addresses and their *sID*. Other considerations was treated in the threat model in the section 3.3.1 p. 80.

4.2.2 K_i^{MCU} establishment

The solution purpose is to develop a security model, based on symmetric cryptography with a suggestion of a scheme for pairwise key establishment at deployment phase.

First, we must deploy network nodes (WBAN and WPAN) by unique and secret identifiers *sID* and register them in the MCU database. Moreover, the MCU establishes a secure connection with the 6LBR to identify the network.

Entity	Description
K_i^{MCU}	Pairwise key between the MCU and the 6LoWPAN node.
K_i	Shared key between the parent node and its children.
K_{ij}	Session key shared between two LoWPAN nodes i and j.
Ke_i^D	End-to-end key shared between a LoWPAN node i and an IP device D.
$Ke_i^{i'}$	End-to-end key shared between two 6LoWPAN nodes i and i'.
S	Generated seed by the 6LBR.
sID	Node unique and secret identifier.
T_s	Timestamp
T_e	Time expiration of the Ts
SEQ	Sequence number

Table 4.2.1: Acronyms used for protocol description

4.2.2.1 Seed generation and distribution

At the starting phase, the nodes must wait for the seed S from the border router 6LBR before releasing anything. The 6LBR generates S and adds to it a timestamp T_s and its time expiration T_e, in order to avoid replay attacks, and to differentiate between an obsolete S of an old session and a new S for the current session. After that, the 6LBR puts S, T_s and T_e it in a package and adds to it a sequence number SEQ to avoid that a single node processes the same message more than once.

The 6LBR sends S to the MCU. As the MCU already has the network nodes $sIDs$, it will use S with the stored sID to generate each node key K_i^{MCU} and store it in the database. At the same time, the 6LBR broadcasts S for all the network nodes (fig. 4.2.1).

4.2.2.2 key generation

When a node receives the message containing the seed S, it checks SEQ number to verify if it is received for the first time or it is already received and used. After, it will check the T_s if it has expired or not. If either of these tests fail, the node drop this message. If the two tests success, it switches to the generation of its own security key (fig. 4.2.2).

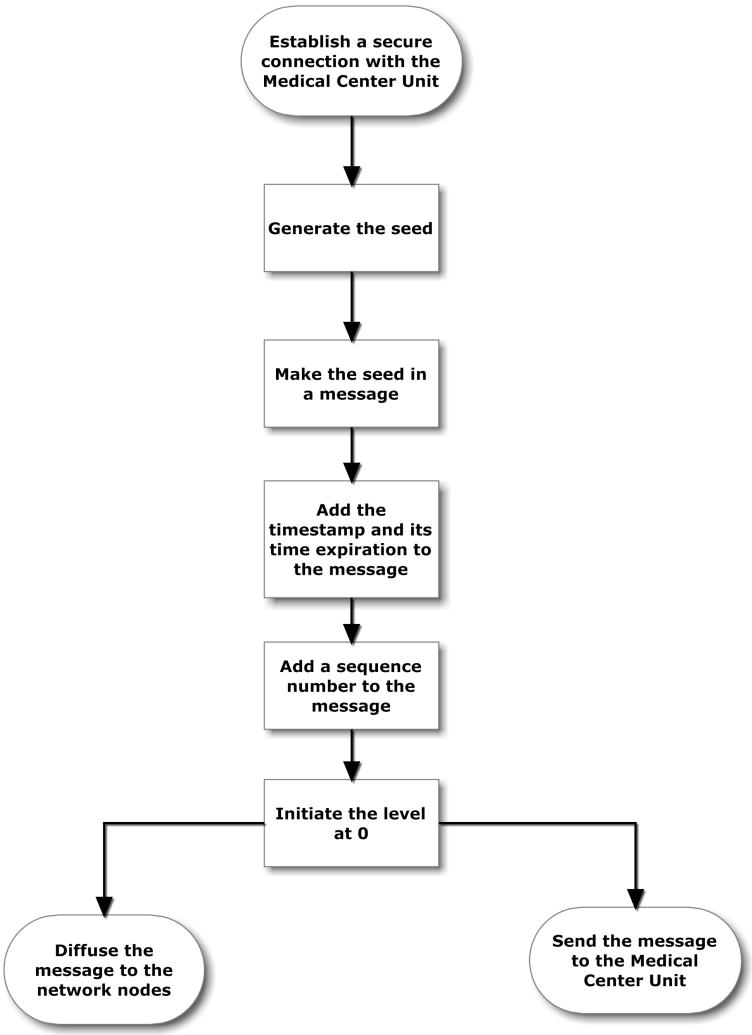

Figure 4.2.1: Seed generation steps algorithm scheme.

When a node receives the correct *S*, it combines it with its *sID* to generate its pairwise key with the MCU. As the *sID* is unique, the key will be also unique.

4.2.2.3 Path building (for WPAN nodes)

Every node that receives the *S* retransmits it to the other nodes that are out of reach of the 6LBR. In the message containing the *S*, there is also another option; the level *L*, which will help to separate nodes in levels and creates the parent-son tree topology where each node in the upper level will be the parent nodes at the lower level, and so on. A node N_i receives this message, keeps the seed and increment the level in the received message as its level, so if the first message that is sent by the 6LBR equal to zero, the first nodes that receive this message will have $L = 1$, and so on, each node that receives this message for the first time will increment its level.

Thus, each node records the one-hop sender address of this message as its gateway to the 6LBR. Nodes shares the *S* so on until all nodes in the network receive it; each one determines its level and its gateway node to the 6LBR.

4.2.2.4 Node authentication

After generating the key, the node must be authenticated within the MCU to verify its authenticity. For this, the node encrypts its *sID* using the generated key and sent it to the MCU via the 6LBR.

At the reception, MCU first identifies the node by its physical address, uses the stored generated key to decrypt the message. If it success to decrypt it, MCU compares the node *sID* received in the message by the *sID* stored in its database, if the two tests success, it will declare the node as authenticated, otherwise, if one of the two tests fail, it begins revocation proceedings (fig. 4.2.3). Revocation proceedings and intrusion detection are explained in the next chapter.

K_i^{MCU} establishment processes is resumed in the algorithm 1.

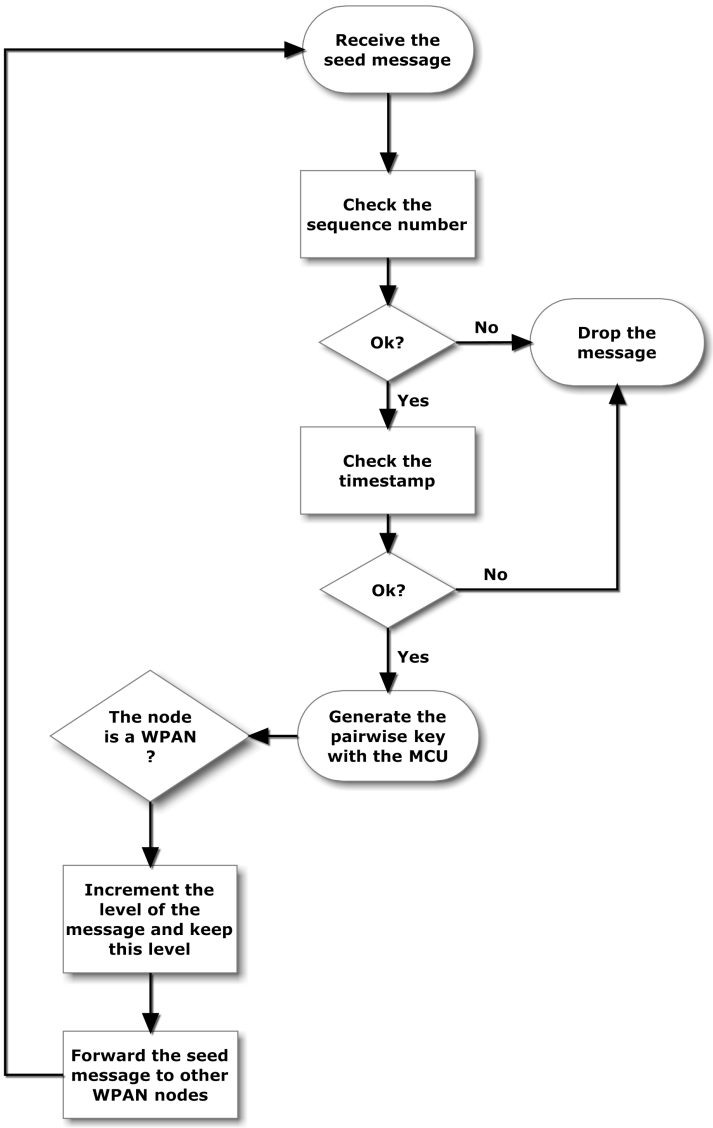

Figure 4.2.2: K_i^{MCU} key establishment steps algorithm scheme.

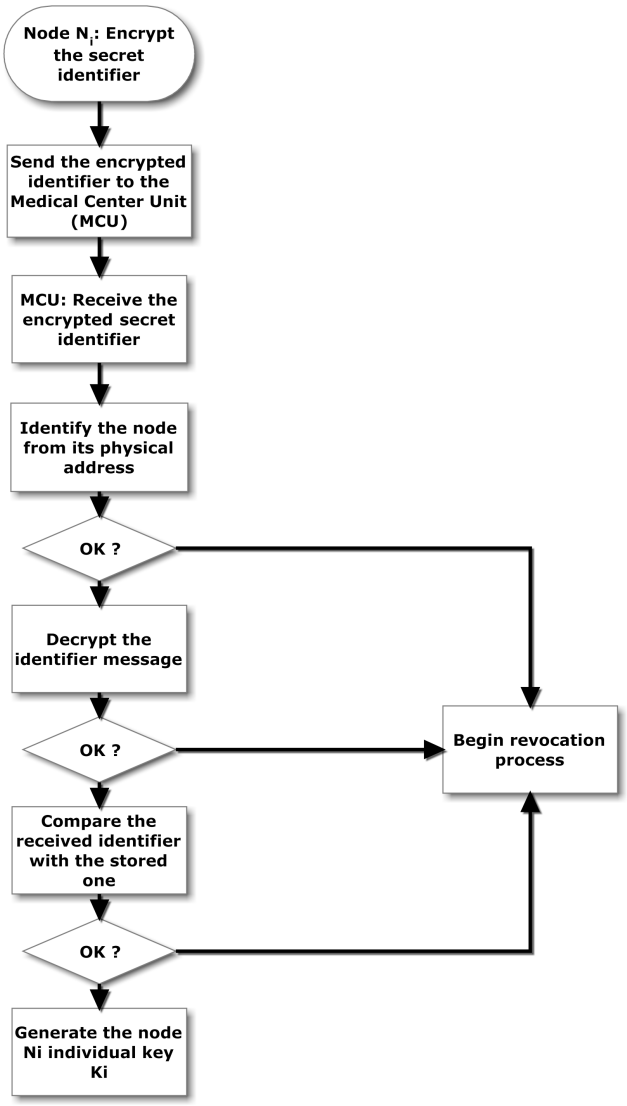

Figure 4.2.3: Node authentication steps algorithm scheme

begin

Step 1: Initiate listening mode.;

if *receives the message M containing the seed S* **then**

go to Step 2;

end

Step 2: Check sequence number SEQ.;

if *SEQ received first time* **then**

go to Step 3;

else if *new SEQ* $>$ *old SEQ* **then**

go to Step 3;

else

Drop M;

end

Step 3: Check the timestamp T_s. ;

if $T_s < T_e$ **then**

go to Step 4;

else

Drop M;

end

Step 4: Increment the level L.;

L++ ;

Step 6: Generate the key K_i^{MCU}.;

$K_i^{MCU} = \mathrm{f}(S, sID)$;

Step 7: Forward M to the other nodes. ;

$N_{i+1} \longleftarrow (\mathrm{M})$;

Step 8: Send the encrypted sID to the MCU for authentication. ;

$\mathrm{MCU} \longleftarrow (\mathrm{sID})_{K_i^{MCU}}$;

end

Algorithm 1: K_i^{MCU} key establishment

4.2.3 K_i ESTABLISHMENT

4.2.3.1 KEY GENERATION

By sending the authentication messages to the MCU, the 6LBR takes this opportunity to save the addresses of the nodes of the network to supply its routing table.

After nodes authentication, the MCU generates an individual key K_i for each node N_i for use in exchanges with the 6LBR and other nodes in the network. This key will also be useful to generate its next session keys without resorting to the MCU.

The MCU will then send each node's key K_i encrypted by its K_i^{MCU}, which will also confirm that the node authentication process went well.

Thus, it provides the 6LBR by these keys, also for that the 6LBR can authenticate the nodes in case of need, it will feed it by *sID* hash of network nodes. Although there has been assumed that the 6LBR will not be compromised, but in our solution we avoid that it has the nodes *sIDs* because if it is hacked, it will be a disaster for the entire network.

4.2.3.2 INTER-LOWPAN NODES KEY ESTABLISHMENT

After establishing primary parent-son relations by establishing routes that connect each node to the 6LBR, nodes will need to communicate to each other. Since they have limited storage capacity, we restrict the sharing of keys between nodes that have a parent-son relationship, and with other nodes only in case of need. The goal is that each parent node N_i shares its key K_i with its son nodes. So each parent node N_i sends the list of the addressees of its children to the 6LBR, which encrypts the N_i key K_i by their keys and sends to them.

Any node can join its neighboring group of one-hop nodes that compose a "family" (a group of children nodes that share the same key of their parent node), we take the example of two neighboring nodes N_i in the level L_i and N_{i+1} in the level L_{i+1}. N_{i+1} sends a request to N_i to join its "family". In order to avoid a DoS attack, N_i records the N_{i+1} address and waits for its authentication, as it warned, each next request from N_{i+1} will be rejected. N_i encrypts the request and N_{i+1} address by its

key K_i and sends it to the 6LBR. When the 6LBR decrypts the message, it will find the request of N_{i+1}, it will understand that N_i wants to share its key with N_{i+1}. After checking the two nodes N_i and N_{i+1} in its database, the 6LBR encrypts N_i's K_i by N_{i+1}'s K_{i+1} and sends it to the latter.

The same method is used between two non-neighboring nodes that belong to the same network, i.e. two nodes that shares the same IPv6 prefix. However, since in this case the communication is temporary and for a specific session, the node receiving the request, supposedly N_i, encrypts the request and the applicant's address, supposedly N_j, by its key K_i and sends it to 6LBR. After checking the nodes, the 6LBR generates a session key K_{ij} and sends to N_i encrypted by K_i and to N_j encrypted by K_j.

4.2.4 *Ke* establishment

4.2.4.1 End-to-end with an IP device

To establish an end-to-end connection between a 6LoWPAN node N_i and an IP device D on the Internet, we will use the MCU as a proxy. We suggest the use of the Host Identity Protocol [168] explained in the section 4.1.2 p. 123 in order to establish a secure end-to-end communication between the MCU and D, its advantages that is self-certifying identifiers; no certificates and trusted third party are required. It provides identifier ownership and makes difference between the identifier and the locator, and supports mobility and IP change as it does not bind to the IP address.

After establishing a secure connection, MCU and D will exchange a secret n using Diffie-Hellman algorithm (section 3.6.1.1 p. 100). After that, the MCU will pass n to N_i encrypted by its K_i^{MCU} to use it to generate its pairwise symmetric key Ke_i^D with the D. Both D and N_i must use the same function with the same parameters to generate Ke_i^D, for that, we will use a hash function.

Normally, both must agree on the hash function they will use to generate the key from the known ones, but since the 6LoWPAN node is resource-constrained, it should use the most optimized hash function. Why in this solution, the MCU

will obligate the D to use the one used by the 6LoWPAN node to generate the key.

4.2.4.2 End-to-end with a 6LoWPAN node

In some cases, a 6LoWPAN node has to communicate with other 6LoWPAN node in an other LoWPAN netwrok, through the Internet in an end-to-end way. For that, they will approximately use the same mechanisms explained in the case of the end-to-end key establishment method between a 6LoWPAN node and an IP device.

It is not necessary that the second 6LoWPAN node belong to a medical network in an e-healthcare system. We consider that the second node belongs to a 6LoWPAN network managed by a remote server RS.

Considering that a node N_i belong to the MCU wants to communicate with another node $N_{i'}$ in other 6LoWPAN network that belong to the RS. Yet, N_i must share a symmetric key Ke with $N_{i'}$, for this N_i sends its request to MCU. MCU establish a secure communication with RS and shares a secret n with it using Diffie-Hellman method. Also, they agree on the hash function that the nodes belonging to their networks will use. Then MCU passes n to N_i encrypted by its K_i^{MCU} and indicate it the method that will use to generate the key $Ke_i^{i'}$. The same will be done by RS with $N_{i'}$.

These solutions are valuable if we replace the MCU by any remote server, local server or even the border router.

4.3 Post-deployment operations

4.3.1 Re-keying

Rekeying contributes in improving the system protection by changing the security keys in a specific time interval. In the case of nodes sharing a pairwise key with the MCU, the rekeying follows the same method explained in deployment phase. For inter-LoWPAN shared keys between nodes, in the case of the parent-son relationship: The parent node generates a new key and diffuse it encrypted by its

current key to its children nodes. In the case of two nodes that need to communicate frequently, after the end of the current session key, or after an order from the MCU in case of intrusion detection, since both nodes already share a key, the first node will generate a nonce no_1 and send it encrypted the second node, which follows the same process by generating a nonce no_2. At the end of the exchange, both nodes combines no_1 and no_2 to generate their new symmetric key. All the old session keys must be deleted after generating the new key, but only after checking that it worked.

4.3.2 Integrity

This objective is to preclude any changing to be made by an unauthorized intruder and to assure that the data coming from the sensor have not been tampered by this intruder.

The CCM mode of the AES algorithm ensures data origin authentication and integrity, by using a Message Integrity Code (MIC) also named as Message Authentication Code (MAC) that is appended to the message. It is created encrypting parts of the data using its generated key of the current session. Upon receiving the message, the receiver will decrypt it and generates the MAC for the received data and compares it with the MAC received in the message, if they match, it confirms that the message is authenticated and has not been altered by an intruder.

4.3.3 Mobility case

We created our solution to deal with mobility, especially for WBAN devices as they are implemented on the monitored person body, which will move from a place to another. As the node is linked directly to the MCU by its symmetric key, even if it changes the network, the service will continue working normally and the data still always secured.

In the case of in a hospital, it will be used many 6LBRs implemented everywhere as gateways. If the patient changes the place, it will change the gateway. In this case, located in the new network, the node sends a join request to the 6LBR' of this new

network containing its sID encrypted by its symmetric key shared with the MCU. We claim that this 6LBR' is already establishing a secure connection with MCU. The MCU authenticates the node, informs the 6LBR' that it is legitimate, and sends to it a seed *S* to generate a new key to initiate a new session.

In the join request, the sensors will include the address of the MCU. So even in the case of the mobile node was found with the 6LBR that was not already established a connection with the MCU, it will find it directly using its address.

4.4 Proposed solution analysis

In each designed security key establishment protocol proposed for resource-constrained networks, it must respect and take into consideration a set of requirements and constraints to be an applicable and effective protocol.

4.4.1 Network model

In our solution, we use the node physical address as its primary identifier, but the node authentication is done using both its symmetric key and its secret *sID*.

As the *sID* will remain secret only in the MCU, an urgent solution in the case of a temporary malfunction of the MCU (it is estimated as a rare case since we must use other secondary MCU servers), the network will continue to operate normally and the data collected will be stored at the 6LBR before restoring connection with the MCU. In the case of the introduction of a new node, as the MCU does not have its *sID* to generate its pairwise symmetric key, it will put it on hold and will inform its neighboring nodes to be more wary in case it is an intruder. If it is the case, it will be treated by the intrusion detection system explained in the next chapter.

4.4.2 Resiliency

Inside a LoWPAN, our scheme supports two types of keys: an individual key for each node, shared with the MCU, and another shared between a parent node and its children nodes. Therefore, in case of a compromised node, it will not affect

other nodes in the network because everyone has a unique key and a unique *sID* that is the basis for the generation of the key. Moreover, only the entire node that belongs to the same group, which is in general and especially in our case a very limited group. In this case, only the data exchanged between the nodes as routing data will be released, not the private patient data as it is secured from end to end.

Thus, most existing solutions are hypothesized no node is compromised or malicious node is introduced during the deployment phase. However, this phase is dangerous because the establishment of routes and recognition of nodes is done during this time. Our scheme takes into account the security of this phase by the designated sharing key mechanism, we use the passive mode where no node starts any process before receiving the seed and generating the security key, no node exchanges sensible information with another before its authentication by the MCU. Thus, no node that its secret *sID* is not recorded in the MCU database will have the possibility to establish a key and join the network.

4.4.3 Scalability

Our scheme is flexible regarding changes in network topology and supports scalability, it suffices that the node *sID* been stored in the database of the MCU to make it able to join the network and establish a connection with other nodes.

If a new node wants to join the 6LoWPAN network, it diffuse a request to all nodes that are close to it. The node that receives this request establishes the same mechanism of key exchange between parent and children nodes. Except in this case since the node is new in the network, firstly, the 6LBR sends it the seed to generate its unique pairwise key with the MCU before it passed it the key of its neighboring node claiming to be its parent node.

4.4.4 Key connectivity

It is determined by the number of keys that every node must have to ensure the stability of communications within the network.

Each node has two different types of keys: the first is a single and unique K_i^{MCU},

the key shared between each node and the MCU. The second type concerns the key shared between a parent node and its children nodes, it is generated by a single node and shared with others. Except upper level nodes whose play only the role of parent nodes, and nodes in the last row that play only the role of children nodes, all other nodes play a dual role at the same time, any node holds its own key that it shares with its children, and the keys of its parents. Since in 6LoWPAN networks, the RPL protocol establishes upward / downward communication where the node communicates only with the nodes of different level of its own, except for an updated topology, a node will not have much of key to store.

4.4.5 Computational cost

The number of encryption / decryption operations is determined by the number of keys that each node can carry. In a LoWPAN, a node N_i, needs three types of keys: the K_i^{MCU} key, the key shared with its parent nodes, and its key K_i shared with its children nodes. So the number of keys that each node can carry equal to 1 + g + p, where p = sum of parent nodes, and g = 1 if a node has children or g = 0 if not.

Concerning encryption operations, the number of computations that each node can perform is: 2 x (1 + c + p) where c = sum of children nodes, and p = sum of parent nodes. Knowing that a node can determine the maximum of parent they may choose as gateway, where the minimum is one node, its main gateway to the 6LBR.

In an instant T, a node communicates only to one router node 6LR; it need others just if there is no answer from the first. In this case, p = 1, the number of computations that each node can perform is: 2 x (2 + c).

Other devices outside the LoWPAN can request a node in an end-to-end communication. If we calculate only the encryption of communication in this case, we obtain 2 x e where e = sum of IP devices communicating with this node. The number of keys will be the number of nodes communicating with this node. However, as the 6LoWPAN nodes are resource-constrained, the number of sessions with external devices must be limited.

These analyzes show that the cost of energy generated by the operations of cryptography (encryption + decryption) depends on the number of connections each node makes, knowing that this number can be limited depending on node's cases.

4.4.6 Storage requirements

Storing keys also depends on the relationships each node has established. In our scheme, a node needs to keep five types of keys. It needs to store one individual key with the MCU, p pairwise keys with its parents, c pairwise keys with its children, and one with its end-to-end correspondent. However, it depends on the type of relationship is that for a long session or for a short session. For a long session, relationships can be identified as follows: the relationship with the MCU, the relationship with a parent node, the relationship with a child node, and relationships with corresponding of neighbors who share with them many communications. What remains for the short session are only relations with corresponding, out neighbors, in need of treatment of an instant request, especially the end-to-end relationship.

So for the long session, a node can hold: number of keys = 1 + p + c + i, where, p = number of parent, c = number of children and i = number of internal corresponding. For the short session: number of keys = i + e, where e = end-to-end node.

4.5 Proposed solution evaluation

4.5.1 Performance evaluation

From energy point of view, which is an essential metric for 6LoWPAN networks, and a critical criterion of choice to adopt or not a solution, our model does not require a lot of calculation or exchange between devices to establish security keys, it can be considered as an energy-economizer.

We use the energy model described in [177] and [178] to analyze the energy cost of the key agreement of our proposed scheme and give an estimation of total energy cost; the energy required for the execution of the cryptographic instruc-

tions and the energy required for transmitting and receiving the used information for key establishment mechanisms, based on estimates for the TelosB platform, since TelosB is more power-efficient than other platforms [179] (MicaZ for example), also, the solutions we chose for comparison all are based on TelosB. We focus only for the energy cost of the 6LoWPAN nodes as the other devices are not resource constrained.

According to the used energy model, the energy required to exchange one bit of data for a TelosB sensor is 0.72 μJ for transmitting and 0.82 μJ for receiving. For cryptography operations, AES-128 algorithm costs 26.74 μJ for key setup, 28.16 μJ for encryption and 322.70 μJ for decryption.

In our scheme, to establish the security keys, a node has to receive firstly the seed S from the border router 6LBR in order to generate its K_i^{MCU} key, which cost 26.74 μJ. In addition, the node has to transmit its secret identifier *sID* encrypted by its K_i^{MCU} to the MCU for authentication.

The first message is the one sent by the 6LBR containing the seed S (32 bits), the timestamp (64 bits), the time expiration (64 bits) and the message protocols header (96 bits), so the total of bits the node receives is 256 bits; that mean it costs 209.92 μJ, plus 26.74 μJ for key setup, that gives 236.66 μJ.

The second one is for authentication, the sensor must encrypt its *sID*, i.e. 28.16 μJ, and transmit a message containing the encrypted *sID* (64 bits), in addition of the protocols header, so it transmits 160 bits, which costs 115.2 μJ, plus 28.16 μJ, that gives 143.36 μJ.

The last one is the message containing the encrypted K_i, the individual key of the node. Firstly, the node decrypts the message, which cost 322.70 μJ. The message length is the same as for the first changing the seed by the key, 352 bits – 288.64 μJ, so the total between the cost of decryption and reception is 611.34 μJ.

For establishing the key K_e for end-to-end communications, a node has to receive the encrypted Diffie-Hellman secret n (128 bits) from the MCU. It is the same as receiving the new key K_i adding to 26.74 μJ for key setup, that gives 638.08 μJ.

We observe that the total cost of the all keys agreement to establish the symmet-

ric keys; in addition of sensor authentication, is 1629.44 µJ, about 1.63 mJ.

We simulate also our solution on the TOSSIM simulator of TinyOS. The simulations were compiled also for the TelosB platform, which is based on the low-power microcontroller MSP430 16-bit with a clock frequency of 4 MHz. It implements the IEEE 802.15.4 transceiver CC2420 with a claimed data rate of 250 Kbps. We used AES 128-bit as the symmetric cryptography protocol. We used PowerTOSSIM plugin for energy analysis. The result is approximately the same; the cost for the total operations was 2.3 mJ.

The result is very interesting and energy efficient compared to other schemes. We only compare our results with the only solutions that have been proposed in the context of the Internet of Things like the hybrid solutions that propose symmetric and asymmetric key establishment; Trust Key Management Scheme for Wireless Body Area Networks (TKM) 28.13 mJ [180] and Lightweight Key Management Scheme for E-health applications (LKM) 17.40 mJ [181]. On the other hand, lightweight public key establishment like distrusted TLS handshake (D-TLS-H) 63.54 mJ, distributed IKE (D-IKE) 40.73 mJ and distributed HIP BEX (D-HIP-BEX) 40.48 mJ [182].

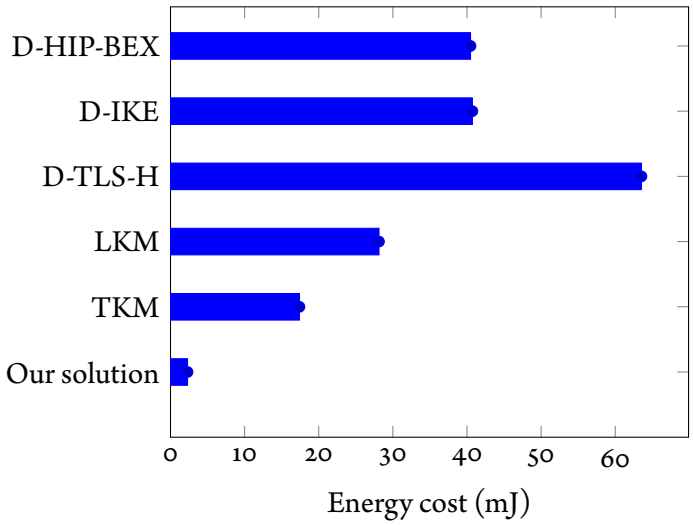

Figure 4.5.1: Energy consumption of IoT key establishment schemes.

There is a huge difference since our solution is totally based on symmetric cryptography, although other solutions are either hybrid, i.e. it uses both cryptography protocols, asymmetric and symmetric. Asymmetric is just used as a basis for sharing symmetric keys that are subsequently used for cryptography. Other solutions are adapted versions of standard patterns of sharing Internet asymmetric keys. Knowing that all these schemes are based on the Elliptic Curve Cryptography (ECC). The figure 4.5.1 gives the result values of key agreement and establishment.

From energy point of view, which is an essential metric for 6LoWPAN networks, and a critical criterion of choice to adopt or not a solution, our model does not require a lot of calculation or exchange between devices to establish security keys, it can be considered as an energy-economizer.

We observe in figures 4.5.2 and 4.5.3 that the power consumption tends to be balanced with the number of nodes to say change there is a slight increase in power consumption with the increase in the number of nodes.

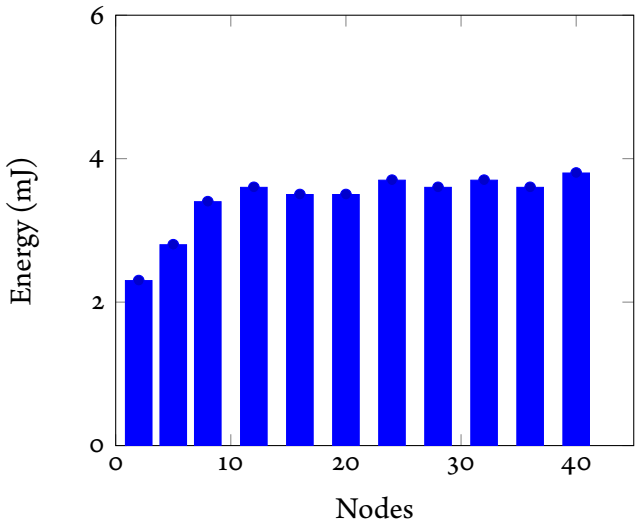

Figure 4.5.2: Total energy consumption.

A linear trend of slight increase is widespread in the energy characteristics of our

system. This is because multiple nodes are involved in key generation activities, key registration and key distribution. Also, the data length has an impact on the energy consumption as shown in figure 4.5.4.

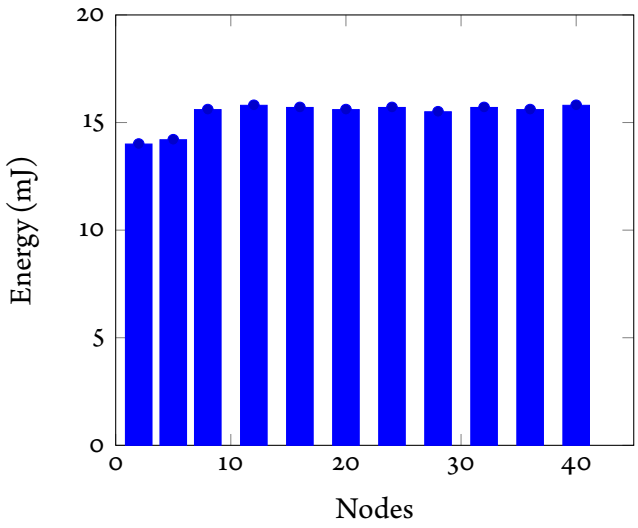

Figure 4.5.3: Total energy consumption (6LBR include).

Our model is based on symmetric cryptography that is recommended by experts in the field as an appropriate solution for LoWPAN networks. Our proposal for key management in our scheme has two key types to secure two important types of communication within this network communication between the MCU and network devices, and communication between these devices, so, any device have to store only its symmetric key shared with the MCU, and the keys of these gateways, i.e. the router devices with a level less than it and convey its messages to the 6LBR. Network device uses its *sID* to establish the key; it does not need to store other additional information that will charge its space storage. In terms of computation, a device only needs to combine between the Seed and its *sID* to have the key, an operation that not require many computation processes.

The time of generation of a symmetric key is negligible. However, the key distribution takes a significant time, with the increase in the number of nodes, the time

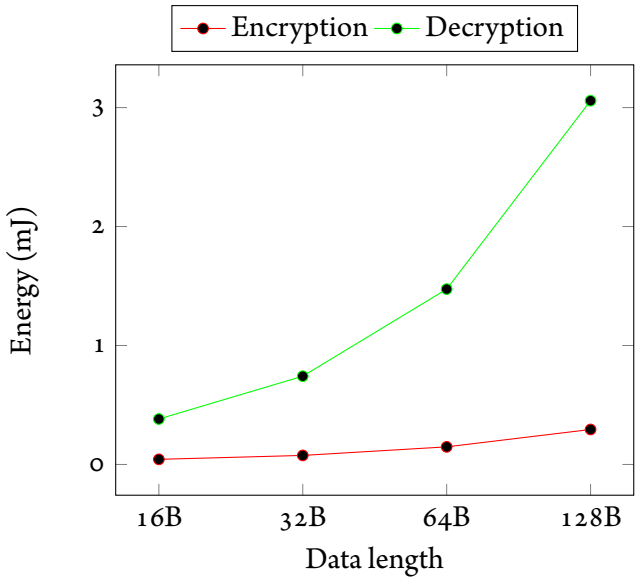

Figure 4.5.4: Data length energy consumption.

spent in key distribution increases linearly, and this makes the graph follow a linear trend as we observe on the figure 4.5.5. Several factors can influence the time of the distribution key as devices gathering, network topology, routing protocol, a device response time, total number of devices on a network, average number of neighboring devices, etc. This will affect any used key distribution protocol. To accelerate time distribution and key management, we used the idea of levels.

During the generation and distribution of keys, the devices need to exchange messages between them, so more than the number of devices increase the more it will take much time, and we fall into a redundancy in processing the same information several times. Separate devices in levels, where each level device communicates only with the upper or lower level devices, will limit the number of communicating to each device and therefore transmit faster the information. Thus, the same information will propagate from one level to another instead of spread from one device to another that will accelerate the distribution of information through the entire network in a very short time.

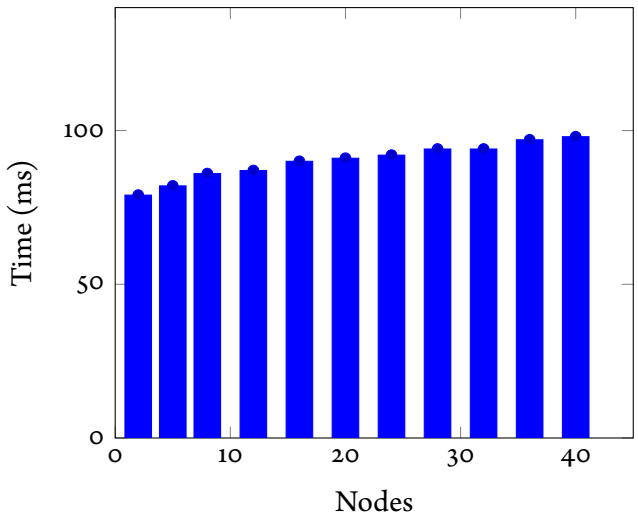

Figure 4.5.5: Key establishment (generation and distribution) time.

4.5.2 Formal evaluation

To prove the fulfillment of the desired security objectives of the proposed systems, we used AVISPA tool [183] to conduct a formal security analysis. AVISPA is a push-button that analyzes the security protocols based on formal methods to check whether the candidate protocol is secure or not. In the case of detection of a vulnerability, it offers the attack track and the step where that was made possible. The tool implements the Dolev-Yao intruder model able to modify traffic passing through, intercept messages, eavesdrop, or insert bogus data.

AVISPA implements four different automatic protocol analysis techniques for protocol falsification: OFMC (on-the-fly model-checker), (CL-AtSe) (constraint-logic based attack searcher), SATMC (SAT-based model checker), and TA4SP (tree automata based on automatic approximations for the analysis of security protocols). AVISPA uses High Level Protocol Specification Language (HLPSL) to illustrate the protocols to be analyzed. It is a special input language used to model the security protocols.

The first step of the verification protocol is modeled using HLPSL official language of AVISPA. HLPSL of the specification language is used to describe the se-

curity protocol as sequences of messages exchanged between the parties and to express desired properties and security objectives. Actors interacting in the exchange are modeled as roles, including their exchange messages with each other. After that, a session is created by binding the roles completely describing the exchange of messages in a given normal operation of the protocol. Other sessions are then specified, with the difference that they comprise an active intruder between different actors, stating its knowledge of option known legitimate entities keys. Modelling intrusion activity is used to find and build interactive attacks on this protocol. Finally, the global environment is created with several parallel sessions simultaneously. HLPSL specification is then translated into a specified format via a description of low-level protocol and given as an input for the four automatic analysis back-ends of the AVISPA tool. Then, verification of security properties of the protocol, namely authentication, integrity, anti-replay and the secret begins. If a property specified security is violated, the back-ends refer a trace explain the sequence of actions that led to the attack and exhibition to have been violated. The result are printed in the SUMMARY; it indicates if the protocol is safe, unsafe, or if the analysis is inconclusive.

We modeled our proposed solutions using the HLPSL to analyze our protocol; we subsquently checked the correctness of the code using SPAN [184]; the protocol animation tool. The HLPSL code is in the annex. The result is:

AVISPA Tool Summary
OFMC : SAFE
CL-AtSe : SAFE
SATMC : SAFE
TA4SP : INCONCLUSIVE

As we see, OFMC, CL-AtSe and SATMC tools have reported that our solution is safe. However, the TA4SP has reported that our solution is INCONCLUSIVE; that is because the case of the existing of compromised nodes in the network, that is clear, cryptography alone cannot provide a complete solution to any system, we have to choose other systems in parallel to solve the shortcomings of cryptography,

such as intrusion detection systems. Indeed, an inconclusive result using an over-approximation in TA4SP does not imply that there exists a real attack.

4.6 Conclusion

Our scheme provides a full solution for securing the 6LoWPAN network while minimizing the use of resources. Knowing that we can optimize more resources by configuring other parameters such as by limiting the number of correspondence of each node.

The cost of computation, communication and storage depends on the relationships that each node sets. With maximum relationships we find that the energy consumed and used storage are still lower than in other solutions, while providing security to communications established by the nodes. Based on these results we can claim that our solution provides optimum scheme for key management. Until the writing of this document, we do not find in the literature a complete symmetric cryptography solution that secures 6LoWPAN networks internal and external communications. Solutions found are adaptation techniques created for sensor networks to ensure security inside the LoWPAN and other lightweight techniques of end-to-end security solutions to ensure network security outside the LoWPAN. Offering a solution to a case independently of other may give an effective solution but it still incomplete since 6LoWPAN network is a complete entity, nodes need to communicate internally with the possibility of establish communications with the external devices through the IP address. Nodes are low resources, combining several separate protocols to establish different tasks will overload the network.

Our solution is based on the protocols used by the 6LoWPAN networks such as RPL and Neighbor Discovery protocol for two reasons: the protocol will be well suited to this kind of network, it does not need adaptation. Also, to take advantage of existing protocols to optimize the cost of using resources. It is based on symmetric key cryptography for all the communications and hence occupies the smallest portion of memory. Overall, we conclude our scheme is scalable and efficient in computation, communication and storage occupation.

Cyber terrorism could also become more attractive as the real and virtual worlds become more closely coupled, with automobiles, appliances, and other devices attached to the Internet.

Dorothy E. Denning

5

Intrusion Detection System

Even when 6LoWPAN has an ideal cryptography line defense, it is still necessary to implement an intrusion detection system (IDS) to deal with threats targeting network performance such as DoS attacks. IDS discover and stop most attacks that make changes on the operation of the network. However, few IDS solution has been proposed for 6LoWPAN networks. IDS missions are to monitor and raise an alarm about any possible threats and pass it to the system to restart the keying process for eliminating the attackers. The security goal is to provide a monitoring system that will attempt to detect anomalous malicious behavior and to prevent it from harming the network performance.

5.1 Related works

For a better precision, we should choose carefully the intrusion detection technique for saving resources and improve the system functions. The techniques are generally divided into two main categories: anomaly-based and specification-based intrusion detection system (IDS). We relied on the following documents [185]-[188] to achieve the analysis.

5.1.1 Anomaly-based intrusion detection system

Anomaly based IDS can adapt to different network environments. However, it usually has a high false alarm rate because of the difficulty in differentiating between malicious nodes and bad behavior. In addition, it needs a lot of time to analyze a large amount of data, where the possibility that an attacker can retrain the system to accept malicious behavior. Between the most used anomaly based techniques are artificial intelligence, statistical, data mining, software engineering and agent-based IDS.

5.1.1.1 Artificial intelligence

The advantage of this method is the ability to extract from the data valued information about malicious attacks, with high precision. Nevertheless, it consumes many resources in data analysis and during training phases. The application techniques are semantic-based, fuzzy logic, game theory and bio-inspired.

5.1.1.2 Semantic-based

In the semantic-based approach, the solutions extract LoWPAN characteristics in order to establish security ontology to construct formal semantics for the network. These established semantics are used as the IDS checking patterns. In the Mao [189], the author defined four layers of the network that are network, semantic, model and cooperative layer, in presenting the relation between these layers as a suggestion for the IDS checking module. Chen & al. [190] transferred LoWPAN

nodes into the ontology concept, to define a relationship threshold; they calculated the relationship of the entire network. This threshold is used as a reference for the node to discover any of its anomaly neighbors. However, these techniques are difficult to build in a diversity 6LoWPAN environment, where the system has different node types and relationships.

5.1.1.3 Fuzzy logic

Choosing the value of the threshold is an important issue in IDS, because if the value is too low, the security will be weak. On the other side, if it is too high, the solution will consume a lot of energy and decrease the network lifetime. For these reasons, the fuzzy logic approach is used for setting a dynamic IDS threshold.

Lee & al. [191] use the cluster nodes number, the key dissemination limit value, and the distance from the base station to each cluster, in order to calculate the threshold. This threshold is diffused periodically by the base station. This technique is well adapted to the topology changes due to the mobility of the nodes, so it can drop false reports. Nevertheless, it requires the base station to calculate the distance toward cluster nodes, which consumes many resources.

Chi & Cho [192] use four factors to calculate the dynamic threshold: the energy level of the node, neighbor nodes list, message transmission rate, and error rate in the transmission. The advantage of this method is its fuzzy threshold easy to be calculated. Nevertheless, the solution is not adapted for different network environment, as the threshold for each parameter is chosen by experiment.

For minimizing the false alarm rate, Parekh & Cam [193] used the probability table and a directed acyclic graph to represent the dynamic site condition in order to calculate the threshold value. The nodes are chosen selectively to assign weights to their sensed reading; therefore, they can improve the detection quality. The inconvenient of this method is its requirements of knowing the network topology and the nodes roles, which decrease the scalability if it is implemented in a 6LoWPAN network.

The advantage of the fuzzy logic approach is that adaptation method with the

environment changes, which improves the accuracy of the network. However, it needs a strong theoretical model in order to deal with different 6LoWPAN network environments.

5.1.1.4 Game theory

The game theory solutions model the security as a game between players with contradicting objectives. The game type can be either cooperative or non-cooperative, zero-sum or non-zero-sum. The objective of this method is to discover the optimized strategies for the players, called the Nash Equilibrium. Dong & al. [194] defined a matrix of simple payoff with IDS probability measures, to protect important nodes in the network against DoS attacks. Estiri & Khademzadeh [195] proposed a repeated game model to detect dropping packet attack, which reward the reputation of the node every time it cooperates, and punish if it does not. After a number of repeated times, the dropped packets average number is shown to reach a stable level and malicious nodes are either to stop the attack. Estiri & Khademzadeh [196] also proposed a Bayesian game to show the interaction between normal and malicious nodes in terms of signaling.

The gaming approach is a powerful and promising to improve the accuracy of the detection. Nevertheless, there are some issues that need to be overcome, such as the players' rational assumption that is not the case in the reality in general, the complexity of modeling the real network and the large workload calculation, which consumes 6LoWPAN network resources.

5.1.1.5 Bio-inspired

Bio-inspired approaches migrate the animal behavior and model these to optimize security solutions. Banerjee & al. [197] combines conventional machine learning and the emotional ants to keep track of the intruder trials. The IDS agent works as the ant agent and later turns to be emotional ant agent to make decisions. The advantage of this solution is the ability to perceive behaviors, deliberate and act according to a principle of self-organization combined with probability values.

Soroush & al. [198] also used a data mining based boosting ant colony for extracting a classification rule set from a network dataset. The entropy and pheromone function are used to direct each tour of the ants, then it continues iteratively to extract a final set of rules. Later, it is used as detection patterns in the larger dataset. This method is an effective way to mine the data; but it consumes resources and time to reach the result.

5.1.1.6 Statistical-based intrusion detection system

Statistical methods identify the threshold model by analyze all the data using different mathematical models, in order to detect abnormal behavior. Among the techniques, there are mathematical model, Bayesian network and the hidden Markov model.

5.1.1.7 Mathematical model

Mathematical approaches use statistical linear or nonlinear models. Phuong & al. [199] used the cumulative sum to detect changes based on the cumulative effect of changes in the random sequence instead of checking each variable threshold. The model is strong, easy to calculate, lightweight and not resource consuming. Nevertheless, the accuracy rate of the model is not very high because the lack of cooperation between the monitored nodes.

Ponomarchuk & Seo [200] analyzed the length of inter-packet arrival time and the number of packets received in a given time window for detecting anomalies in behavior. Speed packet reception was calculated based on the binomial distribution, while the inter time was based on the exponential distribution. The method provides low computation and low cost requirements of memory for storing data. However, the model does not take into account the 6LoWPAN affection environments wireless network.

5.1.1.8 Bayesian network

The Bayesian method is used to calculate an event probability in the future, based on current data. This method is used generally in order to calculate the threshold of the trust model between LoWPAN nodes, so a monitoring node will be considered malicious if it indicates that this value is exceeded. Moreover, Bayesian method clarifies the relationship between the parameters of the network to the attack possibility. When the system has a model of the relationship of reference, it can be said that attack may be initiated from the defect data collected.

In [201], they used Bayesian trust model to calculate the data medium access sub-layer LoWPAN controls to mitigate injustice and consequently on DoS attacks. By adjusting the parameters of the trust model, this solution can be generalized and adapted to other protocols and networks.

Momani [202] combines confidence and data communication trust to infer the overall trust between nodes. The author has shown the need to combine these two values confidences to prevent misleading or break the network threats. The new trust model is represented by Fusion Bayesian algorithm, which combines these two values of trust. The construction of the confidence value for each node is important, it can show the nodes reputation behavior and say it is the malicious node.

5.1.1.9 Hidden Markov model

Hidden Markov model method is similar to Bayesian solution technique. This method can profile the normal and abnormal patterns in the data analysis. Song & al. [203] uses a non-parametric version of hidden Markov models, a hidden Markov models low, to indicate the probabilities of transition rules for the reduction of bearing capacity. The sensing mechanism is performed by the scoring system and deviation alarm. This method has proven effective in the detection of many attacks types, but the error rate is high false positive. In addition, the system still requires a large amount of resources. This should be improved before applying in 6LoWPAN networks.

5.1.1.10 Data mining

The data mining method analyzes machine-learning techniques based on rules. In this method, the system is implemented in a distributed way. It achieves high-precision configuration, but it needs large memory space and high computing power. Some techniques in this regard relates to the classification of data to reduce the IDS analysis work. Xiong & Wang [204] proposed the art support of the vector machine SVM to classify the subset mas function of positive feedback adjustment factor for later use in the optimization of ant colony. The process reduces the subset of function while improving the classification accuracy.

Kaplantzis & al. [205] also used SVM with a radial basis function or polynomial ring to detect the selective transmission and blackholes attacks. Monitoring bandwidth selected parameters are included in a sliding window. This solution reduces the rate of false positives using the SVM technique. Nevertheless, it consumes a lot of resources in computing and communication, which makes it difficult for scalability.

5.1.1.11 Software engineering

The software engineering approaches are in two ways: The software implemented on a server or a host, and the materials used to create a product with its own hardware platform. This approach may improve the standard programming code for the IDS system by using a state machine to track the transition from attack state diagrams and provides a way to monitor system status. This approach is applied in a slightly different purpose: to define a normal behavior in specification-based IDS [206].

5.1.1.12 Agent-based

Agent-based IDS speeds up the operation of the network by dividing the workload by distributed IDS. There are two approaches. Agents divided into autonomous cooperate agents . It provides a more simple and easy system to manage, but it

increases the overhead and causes neck and calculating optimum transmission delay. The other approach is mobile agents, which are moving through the network. It does not create much overhead but suffers from integrity check issue and scan port.

5.1.2 Specification-based intrusion detection system

The specification-based approach can fit well with the principles of abstraction to simplify the selection function and adjust the monitor to its own systems needs. In addition, it may well change and simplifies test operation to determine whether or not a set of events is a violation. It can also take advantage of the knowledge system administrators of potential attacks, and provide accurate detection of attacks with low false alarm rate [207]-[208].

The disadvantages of this method are the lack of ability to define the difference between eligible and illegal behavior and it costs system resources. Moreover, the complexity of the rule may have a direct compromise with performance; also, the system depends on the user's guide in the development of the specification of normal system behavior. The techniques used for these specifications are state machine, machine learning for pattern recognition and statistical analysis to automatically calculate the specifications of the program.

Ning & Sun [209] analyzed changes on AODV operations when attacks occur, which focused mainly on the areas of the two RREQ and RRPL messages. Tseng & al. [210] also analyzed the vulnerabilities on certain fields of the Route Request and Route Reply messages such as ID, hop count, header and sequence number. These vulnerabilities lead to threats such as Tunnelling attack or Man-in-the-Middle attack. Furthermore, Grönkvist & al. [211] added further attacks as the Forged Sequence number and Forged Hop count. Based on these analyzes, they provided different manners of specifying Route Request and Route Reply messages protocol based on the technique of the finite state machine. The main idea is to analyze the received messages to detect transitions of anomalies, which is defined in the identification of threats.

Tseng & al. [212] proposed an OLSR specification that verify the trace and determine the corresponding transition from the last event using an extended finite state machine technique with a backward checking algorithm. Possible change in the fields of Hello and TC messages are also defined. The state transition analysis technique was used to model network-based and host-based intrusions in the network environment. Orset & al. [213] proposed the extended finite state machines that specify the formal specification of correct OLSR behavior, and uses an algorithm to check back to detect runtime implementations violations. The authors have developed semantics to quickly check the specifications.

Mostarda & Navarre [214] specified the operation of the Connectionless Routing Protocol by setting a global automaton based on the properties of basic routing, which should be guaranteed. Based on this controller, the system can then check the status of network nodes. The author mentions two manners to control the transitions, by changing the protocol specification by adding a field in the message that indicates the transition state or sniffing the sequence of invocations to find the unique chain of rules corresponding to the sequence. Some semantic rules have also been defined to simplify the progress of the audit.

5.1.3 Discussion

The IDS systems have become a very attractive research area for intrusion detection. Centralized intrusion detection systems are energy efficient as they are implemented in a powerful node (base station) [215]. However, this solution requires that all sensor nodes are required to submit their data to the base station, which introduce a high communication overload. On the other hand, systems of distributed intrusion detection provides detection performance slightly lower than the previous approaches because they use simple techniques and computationally light detection. In addition, the amount of information exchanged between the nodes is not important, unlike centralized model where all the nodes send their packets to a remote location; the distributed approach therefore is better adapted to the constraints of the resources of the LoWPAN devices.

The hierarchical architecture requires low energy consumption. Apply for a distributed intrusion detection in a topology based on clusters will result in a secure network solution that meets the requirements of LoWPAN nodes.

Our research problem of IDS in the 6LoWPAN network resides on the use of specification-based intrusion detection agent and the location of these agents in the LoWPAN nodes. It is interesting to place the IDS agents optimally in the network to cover the entire network and have a global view of the sensor nodes. This leads to the detection of all packets generated by malicious attackers. We proposed and designed an IDS to counter the most threatening attacks for 6LoWPAN network.

The proposed security approach is applied based on that all nodes in the same group have a similar behavior. We show the performance of our detection model simulation under Tossim and then by an experimental study. We evaluate its performance against several types of attacks. Specifically, we calculate the rate of detection, false positive rate, power consumption for IDS agents to detect attacks (average efficiency). According to the simulation and experimental results, our model has high accuracy of detection, low power consumption and a short time of detection.

A new approach to intrusion detection has recently been proposed for identifying malicious nodes in LoWPAN networks, is based on the fact that nodes that are in the same neighborhood tend to have the same behavior, i.e. the same number of packets sent, received, and rejected, the same signal strength generated. A node is considered malicious if its behavior significantly differs from its neighbors in the same group. These technique has many advantages as it does not require prior training, localized and capable of adapting to dynamics network, also, it has the most suitable mechanism for an encrypted network as a node does not require to analyze its neighbors data to detect their behavior change. Moreover, some attacks in LoWPAN networks can be observed only by the neighbors of the malicious node [216]. The authors in [217] -[220] use this concept to detect a number of attacks in LoWPANs. In all these works, the IDS agents monitor their neighbors to detect internal attacks. Monitoring is to collect intrusion data from messages

sent in their radio range, and then analyze these packets based on selected indicators like packet-dropping rate, the number of transmitted packets and the strength of received signal, etc. However, the common disadvantages of these propositions are analyzing the signals from all the neighboring nodes, which leads to excessive energy consumption, and the strategy of the location of IDS agents in the network is an important aspect and has not been considered in these researches.

5.2 Proposed solution

The basics propositions from the papers that were a source of inspiration for this work are summarized in these solutions; the insider attacker detection scheme [217], the group-based intrusion detection scheme [218], the neighbor-based intrusion detection [219] and Intrusion detection framework of cluster-based wireless sensor network [220].

An IDS system for a 6LoWPAN-based e-healthcare network must satisfy the following properties: simplicity, full network coverage, utility and scalability. In other words, the system would cover all of the nodes in the network, is simple enough to run on limited devices to detect most attacks that would be designed for and it would be possible to implement new mechanisms to detect new types of attacks easily without having to rebuild the existing system.

We propose to build the IDS as powerful global IDS agent running on the border router 6LBR and a lightweight agent running on each node. Global agent has access to information of all network nodes. On the other side, the node's agents can operate with only the information from their neighbors. However, this information is very rich due to wireless nature of communication. Each node upon receiving any message should consider whether it is for the node itself or another node. Then, each node contains information about its neighborhood. For saving energy, It should be possible for a node to turn off its agent to reduce battery consumption.

Symptoms of selected attacks that pose risks of security must be integrated into the node agent detection component. Results of detections are organized in a

database alert data. Nodes are marked as suspicious or malicious there. Finally, a cooperative component can be activated when the communication with other parts of the system or neighborhood is necessary.

The global agent consist of a data acquisition component that collects data from the received packets. These data are processed for further analysis. The processed data is stored using a statistical component. A detection component uses the information stored by the component of the statistics and analysis attacks symptoms.

Our intrusion detection system explores the spatial correlation of neighborhood activities and unlike other systems, anomaly detection, it does not require prior training. The algorithm is localized, which means that information is exchanged only in the limited neighborhood. In addition, apart from the requirement of no prior training, is that it has a pattern that is generic, it is not related to a specific types of attacks. It can monitor many aspects of the behavior of the 6LoWPAN network at a time. The way this is achieved will be described in more detail in the following paragraphs. The basic idea is that in some areas neighboring nodes that are physically close to each other must be taken with the similar network traffic and provide similar values of their sensors. Then it is possible to watch all the attributes for some spatially correlated group of nodes and nominate these nodes, which differ significantly in some aspects as attackers.

We know in a wireless environment, a node N is able to listen to messages coming to its neighbor N_i no matter whether or not it is involved in the communication. The node N creates a model of network behavior of the node N_i as a q-component attribute vector $f(\mathrm{N}_i) = (f_1(N_i); f_2(N_i); \ldots ; f_q(N_i))$ with each component describing an N_i's activity in one aspect. The component f_j represents actual monitoring results of some behavioral aspect of the node N_i for each and fixed j. For example, it might be a measured value from the sensor, the number of dropped packets per a period of time, packet delivery ratio per a period of time, etc. Behavioral aspects are chosen as appropriate and quantifiable properties, which represent statistics that are used to evaluate symptoms of attacks that should be detected by the IDS. The authors in [217], [218] assume that for any local area of normal sensor nodes N_i, all $f(\mathrm{N}_i)$ follow the same multivariate normal distribution.

The data acquisition component of the node N gathers information from its neighborhood and creates the set $F(x) = f(f(N_i)) = (f_1(N_i); f_2(N_i); \ldots ; f_q(N_i))$ of attribute vectors, where $N(N)$ is the set of neighbors of the node N. This set of attributes is broadcast within the neighborhood $N(N)$ and is taken as a source of statistics for the detection component. This approach eliminates the need of the training phase and storing its results permanently in the database of the detection component of the IDS. In each period, the normal behavior of a node is defined as the "center" of the set $F(N)$.

Suspect intruders are considered as nodes, which are far from the "center" of the set $F(N)$ that the threshold θ. Details on calculating of this distance can be found in the cited papers, as well as determining the threshold θ. The final decision about the suspect nodes in our solution is made in the level of the border router, this latter may invoke the MCU remote server for help. Different nodes mark the attacker on the basis of information from different neighborhoods. If a local IDS agent finds a suspect, it alerts the entire group with a warning message about the node. If there are more such messages, the entire group wakes up and all of the nodes monitor the proposed malicious node. If abnormal behavior is detected, the border router is alerted and the actual suspect node is blocked from routing tables until the final decision. The border router revoke a node if it is considered suspect by a majority of its neighbors, and it presents an attack and not just a malfunctioning, after that its excluded from nodes routing tables, reported in the database alert and announced to the remote server.

5.3 Solution description

We propose a new concept detection to identify and prevent different types of attacks in sensor networks. This detection approach is based on specifications, but without the need for continuous updating of rules to maintain the intrusion detection system reliability. We used the concept screened by the works [217], [218] in a hierarchical topology based on the DODAG (section 2.8.2 p. 69). We adopt this method as we demonstrated in the discussion 3.9 p. 113 that the hierarchical

topology is most suitable for 6LoWPAN networks using the RPL as the routing protocol. The following studies [217], [218] proved that the nodes that are in the same group or the same cluster tend to have the same behavior. Since the nodes in 6LoWPAN regrouped in DODAGs, we assume that the nodes are in the same group if they are physically close to each other and tend to have the same behavior. If we have an heterogeneous nodes distributed in the same network where they differ from each other even if they are physically close to each other, in the same DODAG we can make sub-groups of the nodes that are from the same type, i.e. the monitoring node collects audit data about its neighbors but only those from the same type. We have developed a new detection model based on this concept to detect the most dangerous attacks for 6LoWPAN. In the presence of several types of attacks, the proposed intrusion detection approach is evaluated using four metrics; the detection rate, the number of false positives, the average efficiency and the total consumed energy.

In what follows, we describe our detection proposition based on the concept of the normal distribution and detection rules for a set of behavioral change signs in a node. Our goal is to protect the network from attacks aimed at tampering it by detecting the anomaly of the malicious node whatever its type. Each node has an abnormal behavior must be suspect to be an intruder. The final decision should be made following statistical analysis that will confirm if the node is really an intruder or it just present a malfunctioning. The advantage of our approach that it provides flexibility by the detection of new attacks that were not defined by the standards, since it is not tied to a specific type of attack. Subsequently, we present the design of the proposed detection model and its operating principle.

5.3.1 Intrusion detection techniques

Solutions that adopt the concept of neighbor monitoring are based on the determination of the threshold by calculating the mean of the observed phenomena, which means that the node has compared a given phenomenon generated by its neighbor node with a definite value. The result of this comparison is not exact

since the phenomenon is a variable that can take a correct value in a large field, more or less than the calculated mean. This explains the high rate of false negative in these solutions. To deal with that, we adopt a new detection techniques based on the concept of the normal distribution (Gaussian distribution) proposed by [220] to detect attacks and allow a normal functioning of the LoWPAN network.

An observed value can be considered as random and normally distributed. The mean of the normal distribution is then considered as the real value of the observed value, the dispersion of the law then provides information on the error of observation. That is to say, it is possible to calculate an approximate value of the probability that a variable following a normal distribution is in a $[\mu - \sigma, \mu + \sigma]$ around the mean μ. This is to obtain an approximation of the value of indicator observed by considering errors due to changes in the environment or a malfunction.

In a concept of normal distribution, the mean μ and standard deviation σ of the data are calculated. This data is properly distributed if they are within three standard deviations from the average. In our approach, we assume that all nodes that are located in the same DODAG have the same behavior. Therefore, a node is considered an attacker if its behavior differs from its neighbor in the same DODAG.

5.3.1.1 Attacks indicators

We focus in our study about the most known attacks that can be detected by surveying the communications between the nodes and that are detectable only by an IDS. We was based in our study on [221]-[223] to determine the indicators of these attacks in order to determine the parameters to be monitored. We describe in what follows the main indicators.

- Sending ratio (SR): number of packets sent by a node N.
- Reception ratio (RcR): number of packets received by a node N.
- Forwarding ratio (FR): number of packets received by a node N and forwarded by this node to their destination.

- Retransmission ratio (RtR): number of retransmission of the same packet by a node N.

Each indicator shows its efficiency only in protecting the network from one or some attacks but not all, this why each node must take them all in consideration. Wherever there is other indicators, but a 6LoWPAN node cannot monitor them all because it is limited in resources. Therefore, the IDS needs to prioritize the attacks depending on the scenario. We choose only the most important threats that an e-healthcare system need to be protected from it. Our approach is based on cooperation between the chosen indicators to monitor all these priority threats.

5.3.1.2 Behavior monitoring

Behavior monitoring of a node N_i by IDS agent is modeled by the following function: $f(\mathrm{N}_i) = f_1(N_i), f_2(N_i), \ldots, f_q(N_i)$ where q is the number of monitored behavior defined by:

- $f_1(N_i) = \mathrm{SR}$
- $f_2(N_i) = \mathrm{RcR}$
- $f_3(N_i) = \mathrm{FR}$
- $f_4(N_i) = \mathrm{RtR}$

All of these behaviors follow the same multivariate normal distribution in any local area within the DODAG. All values associated with these indicators are in the range of three standard deviations around their mean values. The writing normal distribution function is

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-(x-\mu)^2/2\sigma^2} \tag{5.1}$$

To determine whether the nodes within the same DODAG have the same behavior, the standard deviation σ (5.2) and the Euclidean distance E (5.3) of the

indicators must be calculated. Each IDS agent calculates the standard deviation of the set $f_m(N_i)$, ..., $f_m(N_n)$, i = 1, ..., n, where n is the number of monitored nodes by this agent and m is the selected behavior.

$$\sigma(\oint_m(N)) = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(\oint_m(N_i) - \mu(\oint_m(N)))^2} \tag{5.2}$$

When σ is above a certain threshold θ, the IDS finds that monitored nodes could be an attacker. To determine the node that has a malicious behavior, the IDS agent calculates the E of $f_m(N_i)$ in the center of the set $f_m(N_i)$, ..., $f_m(N_n)$, given by calculating the mean μ of its components. When E is above a certain threshold θ, the node is considered as an attacker.

$$E(\oint_m(N)) = \oint_m(N_i) - \mu(\oint_m(N)) \tag{5.3}$$

knowing that:

$$\mu(\oint_m(N)) = \sum_{i=1}^{n}\frac{f_m(N_i)}{n} \tag{5.4}$$

Our goal in this solution is to provide a reliable mechanism for detecting intrusion in terms of attack detection and lightweight in terms of computation process and communication, i.e. obtaining a low overhead. Therefore, our detection mechanism is mainly based on the concept that all nodes in the same DODAG should have similar behaviors. These behaviors are represented by the noted indicators previously described. In our solution, we used a hierarchical architecture based on the DODAG topology.

5.3.2 Intrusion detection agents

In our scheme, each node has the ability to enable its intrusion detection agent. When a node performs the heavy calculations, it can disable detection to conserve energy for a while. For the analysis and detection process, we propose two detection agents: node IDS N_{IDS} and global IDS G_{IDS}, located respectively at the nodes

and the border router 6LBR. The first applies a detection based on the behavior of neighbors to identify malicious nodes. The second aims to reduce the number of false positives that occurred when the N_{IDS} agents suspects a normal node as an attacker. WBAN nodes will not hold any IDS agent, the N_{IDS} agent will be located on the gateway device, this agent will monitor the WBAN devices considering them as its neighbors.

5.3.2.1 Node IDS (N_{IDS})

The strategy of the location of N_{IDS} agents in the network is a very important point, since the increase of the number of agents in a network leads to a communication and calculation overhead, and therefore a decrease in the lifetime of the network. An important point already mentioned is that the density of nodes used in e-healthcare applications is low since it is limited in space, for this, the N_{IDS} agents will be implemented in all the network nodes. Our solution is that each node is monitored by its one-hop neighbors in the DODAG as they are intended by its messages and because they are in its radio range. Therefore, this strategy leads to detect all malicious nodes with low overhead (fig. 5.3.1).

The N_{IDS} has the following missions:

- *Data collection*: it is responsible for collecting packets in the radio range of N_{IDS}, storing the physical address of the analyzed node and calculating indicators behavior, is related to each node.

- *Detection*: it aims to implement the policy of detection based on the fact that in each DODAG, the indicators behaviors should follow normal distributions. The N_{IDS} agent monitors its one-hop neighbors by calculating the standard deviation and the Euclidean distance of their behavior.

- *Prevention*: when abnormal behavior occurs, the N_{IDS} sends an alarm as a message to the G_{IDS}, so that it can confirm the malicious nature of the suspected node. This alarm message includes the suspect node (physical address) and detected indicator type. In this case, the G_{IDS} receiving such a

message will trigger an alarm counter. When this counter reaches a certain threshold, the G_{IDS} will make a final decision.

5.3.2.2 Global IDS (G_{IDS})

Each GIDS agent has the following missions:

- *Data collection*: it receives an alarm message from N_{IDS} agents. This message contains the suspect node and detected symptom.
- *Decision*: G_{IDS} stores the address of the suspect node in a database (blacklist) and increases a specific counter of malicious nodes. The latter is calculated as the number of times N_{IDS} agents within the same DODAG identifies a node as malicious. When this counter exceeds a threshold, the corresponding node will be ejected from the network. When the G_{IDS} identifies a node as normal and the N_{IDS} agent detects it as malicious one, the G_{IDS} stores the address of the N_{IDS} in a blacklist and the counter associated with this agent is increased. When this counter exceeds the threshold, this N_{IDS} will be designated as the intruder who tries to tamper the network by false information, it will be ejected when the other N_{IDS} agents identify it as a malicious node and the G_{IDS} affirmed that decision.

5.3.2.3 Communication activities between IDS agents

In LoWPAN networks, the communication process requires a large amount of energy compared to the process of calculation. Therefore, our detection approach aims to reduce the cost of communication between agents of intrusion detection to increase the lifetime of the network. This is achieved by minimizing the amount of information exchanged between N_{IDS} agents and between N_{IDS} and G_{IDS}. The N_{IDS} sends two types of messages: the first is for the G_{IDS}, the second to all N_{IDS} agents that are located on its radio range. They contain the address of the suspect node and the type of detected attack.

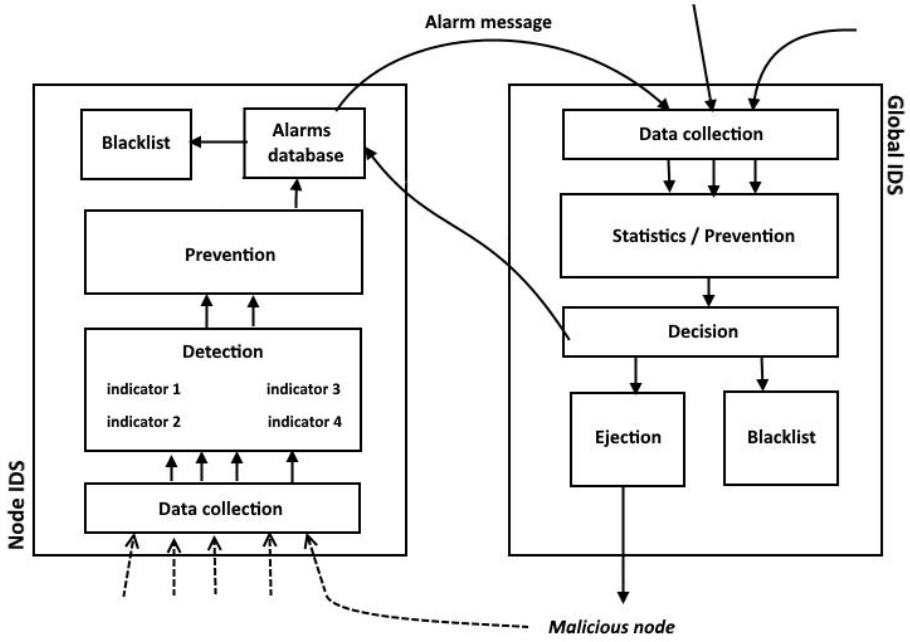

Figure 5.3.1: Intrusion detection agents architecture.

In addition, the mechanisms of cooperation between IDS agents can be classified into two approaches: Each IDS agent exchange intrusion data with other agents. This approach generates high communication load. Each IDS agent works with its neighbors agents to make a final decision about the suspect node (intruder or not). In this approach, the IDS agent only sends an alarm message to its neighbors, where the length of the message is much smaller compared to the previous approach, which indicates a low communication load. Accordingly, our detection scheme is based on this cooperative approach to detect malicious nodes with high accuracy and low power consumption.

Cooperative approach is used for the information exchange between IDS agents running of different nodes. When network density is low and there is not enough nodes monitored by a single IDS agent, it is helpful that an agent collaborates with its one-hop neighbors; the neighboring nodes exchange the information about the suspect nodes they have gathered. Alternatively, this can be done among nodes that are two or more hops away from each other, but we limit our solution to one-hop to reduce the number of monitored nodes and also, in order to reduce false alarms as some indicators may differ only if the monitor node is far from the other. The IDS agent would not extend the number of nodes it is monitoring but only refine the information about them. The result of these cooperative information are sent to the G_{IDS}. These information will help it as data for its statistical technique that used for analyzing the relationship between the received alarms from the network G_{IDS} for potential threats. Evaluating only one indicator of a suspect node behavior can be seen normal in given range; but, evaluating alarm messages in a combined manner can indicate a threat.

5.3.3 Intrusion detection modules

In order to establish a system adapted to the distributed nature of 6LoWPANs networks, we have designed a distributed detection system. It locates nodes with abnormal functioning by listening to the traffic. After treatment, it decided to discard the package or transmit it to the next hop. Each node that receives a packet from its

neighbor node, it treats it in two modules: local control and data collection. The local control module verifies the legitimacy of the neighboring node sending the message. If this is the case, that mean that sending node is not reported malicious, the node processes the packet and perform other normal tasks. At the same time, the data collection module interprets the header information to be used by the intrusion detection system. The interval of the threshold already determined, if the result of the treatment is different from the predicted value, an alarm is generated, the node is declared abnormal and action must be taken to detect if it is malicious or just a dysfunction.

5.3.3.1 Local control

The local control unit the audit engagement and validation of received packets. It verifies the identity of the sender and decides to reject the package or transmit to treatment. This module listens systematically all communications that took place in the radio field. He decides for each packet to treat or reject it. It deals only with packets received from one-hop neighboring nodes, from its children or its parents. The intrusion detection processing will take place only if the sending node belongs to this category, and it is not reported as malicious.

5.3.3.2 Data collection

Generally, sensor nodes listen jumble communication exchanged between neighboring nodes residing in its radio range. Since 6LoWPANs nodes have very limited memory and storage space, the data collection unit will not store data, it will be limited to listening to the data and transmit them to the processing unit.

This unit acquired the information required by interpreting the header. The detection strategy is applied once the data is being processed. If the result shows a different level of the predicted value, an alert is issued. After collaboration with neighboring nodes, the local agent says the node as normal or abnormal. Results are sent after the overall agent to determine if the node is malicious to take the necessary measures against it.

5.3.3.3 Intrusion detection

A number of rules have been chosen to detect a variety of attacks that are determined by the established indicators to set their thresholds after the normal execution of the 6LoWPAN network. As explained in previous sections, the threshold values are set using the normal distribution. These rules are represented as follows:

- Low: if the value of the result is below the minimum "μ- "σ, in the case where it has an attack pattern.
- High: if the value of the result is greater than the maximum threshold "μ+ "σ, if it has any attack pattern.
- Normal: if the value is between the minimum and the maximum threshold, but it shows no attack pattern.

5.4 Proposed system evaluation

5.4.1 Performance evaluation

In our study, we use the TelosB in Tossim simulator as we did on the previous simulations of the security keys establishment, in order to evaluate the performance of our model in terms of the detection rate of true positive and false positive rates. IDS works well should have a false positive rate near to 0% and a very high rate of detection rate. According to these metrics, we determined the optimal detection thresholds for each attack (relative to the standard deviation and the Euclidean distance) to meet the requirements of our target. Subsequently, we simulated our model to assess experimentally the average efficiency resulted in the time required for IDS agents to detect all attacks in the network, the number of true positives and the number of false positives. In addition, we evaluated the total energy consumed during the execution of our model. In what follows, we present the simulation results of our detection model.

5.4.2 Attacks indicators

A 6LoWPAN network can undergo several types of attacks as we studied in the previous chapters. In our solution, it is not intended for a specific attacks as explained, but our approach is based on the study of the normal operation of the network indicators, their disturbance will indicate the network exposure to an attack whatever this attack.

A number of malicious nodes was randomly chosen from all scenarios. We chose to implement the most known and most dangerous attacks for the test; these attacks are "hello flood", "blackhole", "sinckhole", "wormhole" and "selective forwarding". The threshold is obtained after running the simulation for 15 times in each case.

Unlike other studies, we integrated cases of normal nodes that have a malfunction or behave differently in a given time.

5.4.2.1 Sending rate

In a kind of attack, the attacker sends a large number of packets, so the sending rate among attackers nodes is high compared to others. Figure 5.4.1 shows an analysis of the sending rate, we note that the average packet forwarding among attackers nodes is very large compared to normal nodes.

5.4.2.2 Reception rate

In some type of attack, the attacker aims to get a large number of packages, so the receiving rate for this node has very high average. Note that the number of nodes was increased relative to other nodes. Figure 5.4.2 shows an analysis of the rate of receipt of the network nodes; we see that the nodes that have been selected to carry out such attacks receives a greater number of packets than other nodes.

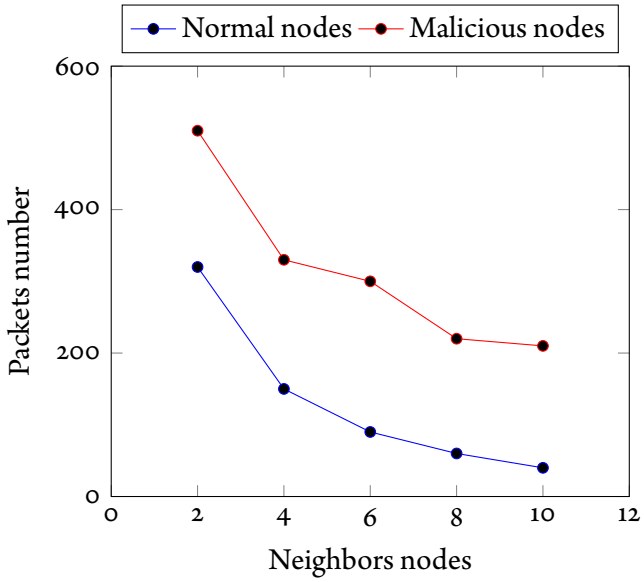

Figure 5.4.1: Sending rate analysis of normal nodes and malicious nodes.

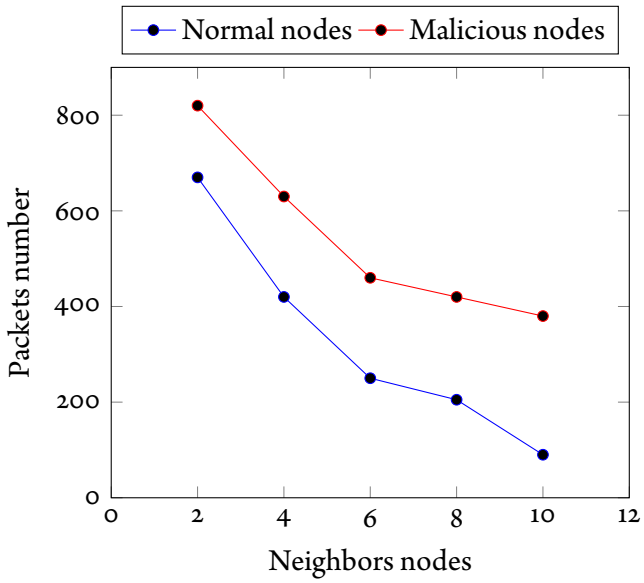

Figure 5.4.2: Reception rate analysis of normal nodes and malicious nodes.

5.4.2.3 Forwarding rate

There are attacks that aim to disrupt information exchanged in the network, like the non-forwarding of some packages, which generates false information. The attacking node records a lower average packet transfer to other nodes. Figure 5.4.3 shows an analysis of the data rate; we note that the average forwarding of malicious nodes is less than that of other nodes.

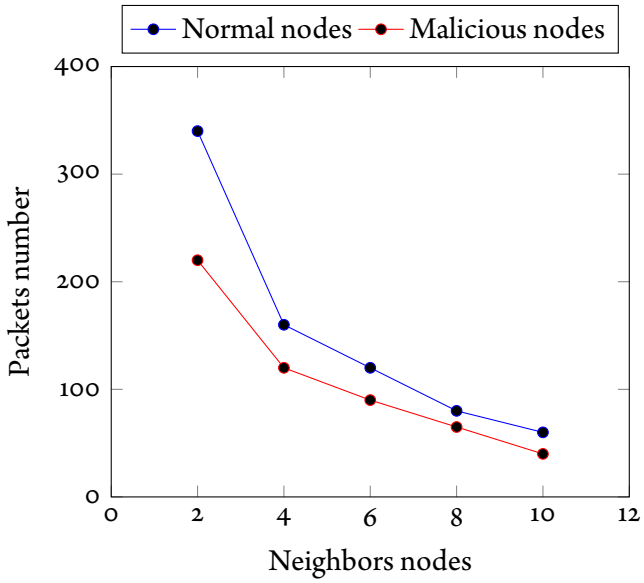

Figure 5.4.3: Forwarding rate analysis of normal nodes and malicious nodes.

5.4.2.4 Retransmission rate

Unlike previous attacks, a kind of attack aims to retransmit the same packet multiple times. Therefore, the transmission rate of the attackers is much more important than the other nodes. Figure 5.4.4 shows an analysis of the transmission rate; we note that the average retransmission among attacker nodes is more important than the other nodes.

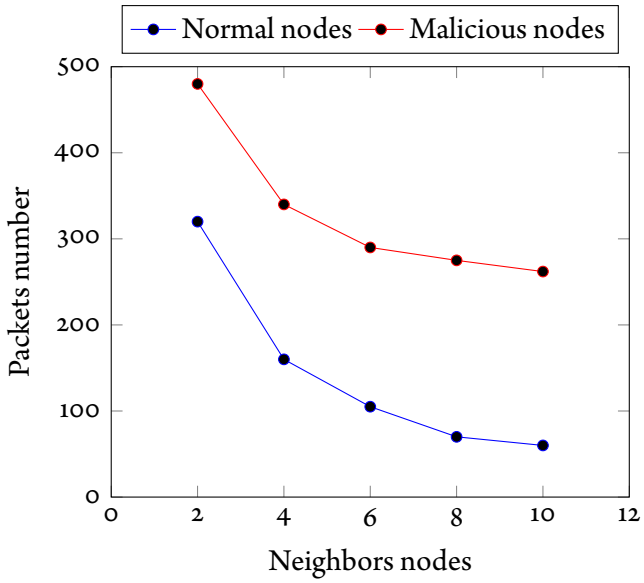

Figure 5.4.4: Retransmission rate analysis of normal nodes and malicious nodes.

5.4.3 Simulation

We considered in the simulations of a network of sensors with 40 static nodes deployed in a random manner in a square area of 100 x 100 m². The simulation time was for 800 seconds.

In the approach, where the N_{IDS} agent determines in its radio coverage as an indicator of a neighboring node does not follow a normal distribution, the Euclidean distance on this behavior is calculated to detect the suspect node execute an attack.

Our results show that IDS is running efficiently and accurately with a very low false positive rate of less than 10% and a high of true positive rate more than 90%. Moreover, nodes generally consume less energy.

As illustrated in the IDS model performance graph, the detection rate is almost 94% when the number of nodes IDS is high (more than 10 agents). However, we have noticed an increase in energy consumption when the number of nodes exceeds 20 IDS agents.

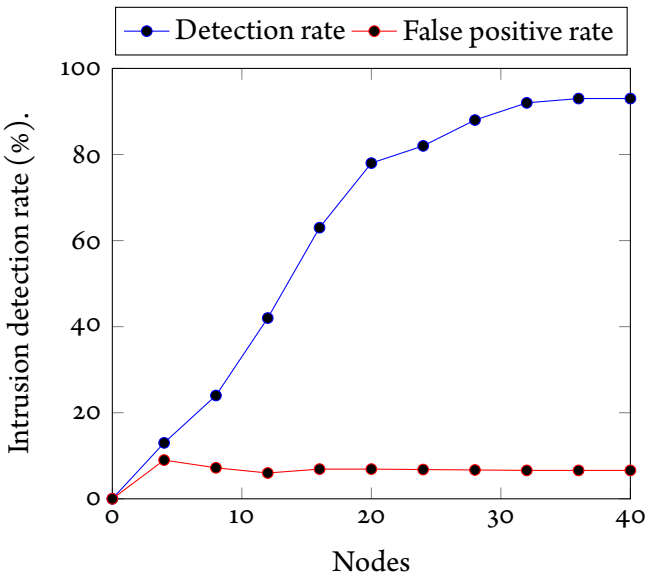

Figure 5.4.5: Intrusion detection rate.

The combination of the detection based on indicators and the collaboration between nodes allows the model intrusion detection to achieve a high rate intrusion detection with a very small number of false alarms, when the number of IDS is large (i.e. greater than 10 agents).

Thus, the use of our approach based on the normal distribution for intrusion detection can meet the requirement of the application in terms of detection rates of attacks and number of false alarms generated by IDS agents.

5.4.4 Energy consumption

About the energy, from energy consumption graph in the figure 5.4.6, it is clear that our detection model has low power consumption. This improvement is achieved by the fact that IDS agents generate a low charge of communication and computation (low overhead communication and computation). In addition, our detection modules involve energy consumption less than the techniques proposed in previous work, based on the core protocols of the 6LoWPAN network and limiting

the number of monitored nodes, and the context of our application implies a low density of nodes, which also has impact on energy consumption. Yet our detection frame has been evaluated and it has been shown to be effective, even when the density of the network is high. Therefore, we can say that our model improves the detection of network lifetime.

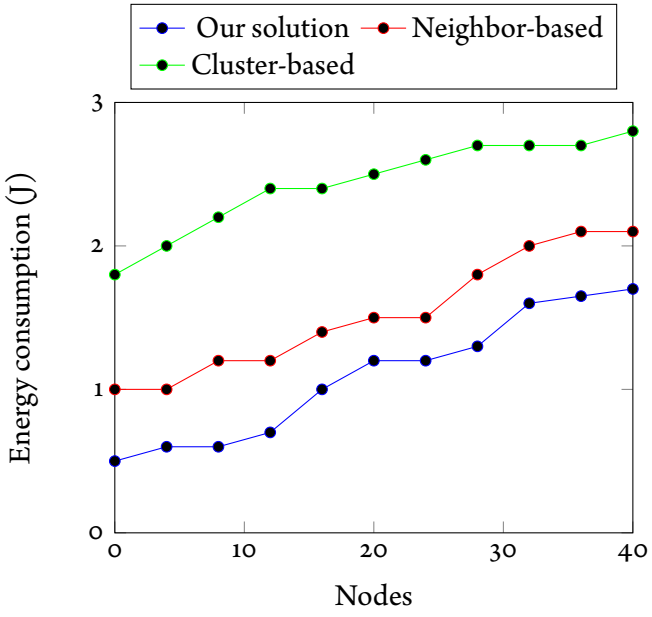

Figure 5.4.6: Energy consumption evaluation.

5.5 Conclusion

We proposed a new detection approach based on behavioral concept of neighboring nodes. This is a new intrusion detection approach was recently proposed for the identification of malicious nodes in LoWPANs networks, it is based on the fact that the neighbor nodes tend to have the same behavior, that is to say, the same number of packets transmitted, received, and rejected, the same strength of the generated signal, etc.

In addition, we have applied this concept to detect attacks that can cause significant damage in 6LoWPAN networks. In our approach, we assume that all nodes that are located in the same group have the same behavior. Therefore, a node is considered a potential attacker if its behavior differs from its neighbors in the same group.

We focus in our study about the most known attacks that can be detected by surveying the communications between the nodes and that are detectable only by an IDS without considering specific attacks. We determined the indicators of these attacks in order to determine the parameters to be monitored.

Our IDS research in 6LoWPAN networks was in the use of intrusion detection policies by IDS agent and the location of these agents in the network nodes. In the first, two major detection techniques have been proposed in the literature; signature-based and anomaly-based detection. Each technique has advantages and disadvantages. Our idea was the use of the advantages of these techniques to counter the attacks with a maximum load limit of computing and communication generated by IDS agents. In the second point, we tried to place them optimally in the network to cover the entire network and have an overall view of the sensor nodes. This leads to the detection of all malicious packets generated by the attackers.

Conclusion

Securing medical confidentiality in the Internet of Things based on 6LoWPAN networks is a challenge. Indeed, a LoWPAN network in general is a hostile environment, which brings several security challenges, due to its characteristics and specificities (ad hoc networks, limited capacity, resource constraints, etc ...). At these security constraints, there are the vulnerabilities of its integration to the Internet, by its nature, a world filled of several threats in different forms. The deployment of 6LoWPAN networks in healthcare applications also induces new events to be considered when designing a solution to the security challenge.

The treatment of our work is divided into five chapters besides the introduction and the conclusion, we have clarified the state of the art in terms of Internet of Things applications in the healthcare field, more precisely the 6LoWPAN networks, after an exhaustive analysis of security-related needs where we defined the main issues on which it relied to establish appropriate security solutions. We have proposed two solutions to this end, a key management system as a first line of defense and an intrusion detection system as a second line of defense.

Chapters summary

We started in the **first chapter** with a discussion of the challenges brought by the transition from the traditional Internet to the Internet of Things. We have introduced the concept of the Internet of Things and how e-healthcare applications take benefit. We also reported an introduction to detection devices; wireless sensors,

their operation and constraints.

We explained that the purpose of the creation of the Internet of Things and the development of its mechanisms is to empower independent devices and the direct control of the human user, and to enable it to monitor and control remotely these devices. The other objective of this development is to get more opportunities in Decision Support Systems. The Gold Standard of the Internet of Things is the huge impact it will have on many aspects of life and daily behavior of potential users. We have also introduced in this chapter the technology 6LoWPAN (IPv6 Low power Wireless Personal Area Networks). We explained the context in which the IETF 6LoWPAN developed the technology to enable these devices to connect to the Internet, and make the concept of the Internet of Things a reality.

We discussed how the Internet of Things will offer many interesting opportunities in several areas: industrial and structural monitoring, environmental monitoring, automotive, automation, etc., but nowhere it offers greater promise in the field of e-healthcare, where its principles are already applied to improve access to care, improve its quality and reduce its costs. The e-health applications are designed to improve existing health services and improve the techniques of remote monitoring, especially for people with difficulties such patients at risk, the disabled, the elderly, children and the chronically ill. Automating the collection of data reduces the risk of human error, caregivers in this case will provide reliable information about the patient with a negligible error rate. This will improve the quality of diagnosis and avoid human error during collection or transmission of information, which can have a harmful impact on the patients' health.

We have dealt in the **second chapter** with the 6LoWPAN technology by determining its mechanisms, the challenges faced and the requirements for its application in the field. We analyzed the different solutions that have been proposed to address these challenges.

The 6LoWPAN networks are created by connecting islands of wireless sensor devices where each island has an end network on the Internet. It is a network that IP packets are sent to or from its destination, but that does not act as a gateway to other networks. The 6LoWPAN architecture consists of a single or a set of LoW-

PANs. To obtain a 6LoWPAN network, we must have a LoWPAN network that combines between two types of limited resources devices opting an IPv6 address: host and router. The host device is the endpoint of the network, and the router acts as a link between the endpoint devices. This devices separation are established in agreement with the division proposed in IEEE 802.15.4 which divides devices into two types: FFD (Full Function Device) or RFD (Reduced Function Devices). These nodes communicate with each other wirelessly via Ad Hoc mode, i.e. without any infrastructure and they share the same IPv6 prefix. Regarding communication with other IP networks, it is established through the 6LoWPAN Border Router (6LBR). The 6LBR is a powerful machine, responsible for determining the IPv6 prefix and its distribution to nodes, assumes the role of the LoWPAN monitor and the controller, regulates sent and received packets traffic, supports header compression and manages the operations of the Neighbor Discovery Protocol (Neighbor Discovery). Each node in the LoWPAN must register in 6LBR database.

Regarding routing, 6LoWPAN network has introduced new concepts and measures that are not addressed by other standard routing protocols in wireless networks. A new IETF working group was created under the name ROLL (Routing Over Low power and Lossy networks) to meet the requirements of routing due to the implementation of the new adaptation layer (layer 6LoWPAN) in these networks. The IETF-ROLL working group proposes the RPL routing protocol (Routing Protocol for Low power and lossy networks) based on the concept of the DAG (Direct Acyclic Graph) to avoid creating loops in the tree constructed by the distance vector algorithm. RPL has the ability to build multiple return paths to the same destination and defines alternative routes when default roads are inaccessible. This protocol will target resource-limited networks in terms of energy, power, and bandwidth, characterized by a high packet loss probability and a very high error rate.

In the **third chapter**, we studied the security issue in 6LoWPAN networks and we have provided a detailed analysis of all it aspects, objectives, threats, attacks and proposed solutions. In each section, we have summarized the main requirements

that must be faced in order to design a security system complies with 6LoWPAN networks for e-health applications.

We explained that the 6LoWPAN threats can be divided into two categories. Those who seek to violate the confidentiality, authentication and integrity of the network, and those who aim to break its performance. Our goal is to provide security via an encryption system that protects network data and a control system that seeks to detect malicious abnormal behavior in the network operation and prevent harm to the performance. Our main challenge in designing a security system for 6LoWPAN network was to select optimal techniques to be adapted to the resource constraints of its aircraft.

We have considered the findings of the analysis from this chapter in order to avoid the shortcomings of existing solutions. We proposed an intrusion detection system that protects the features and availability of 6LoWPAN networks and simultaneously provides the security of internal and external communications network, where most of the existing solutions focus only on one of these two. Although our solution is designed for e-health applications, it can be adapted to other areas.

In our previous study, we found that symmetric cryptography is most appropriate for 6LoWPAN networks over asymmetric cryptography, because it does not consume a lot of energy, it is fast and the key size is small. However, the major problem with this type of cryptography is key establishment, where in particular apparatus of 6LoWPAN networks will communicate through the Internet with other strange devices; that do not share them with no set information. We provide a key management system for symmetric cryptography that provides a comprehensive solution safe and energy efficient.

Thus, regarding the Intrusion Detection System (IDS), we have established a set of requirements that IDS must meet, such as the preservation of power transmission, which minimizes the data exchange between nodes, minimizing the impact of a possible attack in critical applications, run in real time, monitoring of neighbors, and stand in a distributed manner based on the cooperation of IDS agents. We designed a system that meets these requirements while providing a high level

of intrusion detection and low power consumption.

The **fourth chapter** presents our first line of defense; the establishment of cryptographic key system. We designed this system to provide a solution for the key establishment in 6LoWPAN networks to ensure its security, taking into account the performance requirements like energy optimization, scalability, flexibility, mobility and connectivity. Our solution offers three types of security keys: a key pairs between the medical system unit (MCU Medical Center Unit) and each node on the 6LoWPAN network, shared group key between a parent node and its child nodes, and end-to-end session key between a 6LoWPAN node and other IP device on the Internet. We also provide a detailed evaluation of the results from the standpoint of security and energy consumption, which proves the effectiveness of our proposed approach.

Based on the results of our experiments, we demand that our solution provides optimal diet for key management. Until the time of this writing, we did not find in the literature a complete symmetric cryptographic solution that secures internal and external communications of the 6LoWPAN network. Most solutions are coping techniques created for sensor networks to ensure security within the 6LoWPAN and other minor technical solutions from end-to-end to ensure the security of communications outside the 6LoWPAN. Offering a solution to a case independently of the others can provide an effective solution, but it is incomplete for 6LoWPAN networks that exhibit a complete entity, nodes need to communicate internally with the possibility to establish communications externally through the Internet. Since the nodes have low resources, made to combine several separate protocols with one goal, which is the network security, will overload the nodes and the network.

The **fourth chapter** and last one presented the second line of defense; intrusion detection system (IDS). We proposed a new detection approach based on monitoring the behavior of neighboring nodes. It is a new intrusion detection approach was recently proposed for identifying malicious nodes in networks with resource constraints. It is based on the fact that the neighboring nodes tend to have the same behavior, that is to say, the same number of packets sent, received, and rejected, the

same strength of the generated signal, etc.

We proposed to establish the IDS as a powerful global agent that runs at the base station and a lightweight agent running on each node. The overall agent has access to information for all network nodes. On the other hand, local agents at nodes monitor their neighbors. Its main objective is to detect misconduct malicious nodes and launches an alert to the base station. The results show that the proposed system is able to withstand attacks effectively and with less power consumption.

Our IDS research problem in 6LoWPAN networks was in the use of intrusion detection policies and the location of these agents in the network nodes. Two large detection techniques have been proposed in the literature; signature-based IDS and anomaly-based IDS. Each technique has advantages and disadvantages. Our idea was to use the benefits of these defense techniques with a maximum load limit of calculations and communication generated by IDS agents. Thus, we have tried to place them optimally in the network to cover the whole network and have an overall view of all nodes. This led to the detection of all malicious packets generated by the attackers.

Solutions limits

Unfortunately, nothing is perfect, as regards the limits of our contribution, we can mention:

- The security needs differ from an area to another and from a context to another, so any proposal of a security management will be limited to its scope.
- If we want to generalize our solutions to other applications, it is estimated that it is optimized for Indoor Wireless Sensor Networks such as smart homes applications.
- Due to resource constraints, we limited our IDS system to a specified number of indicators. Which can leave escaped other threats.

- Thus, very few researchers are working on security in a large-scale sensor network, because it is difficult to implement and manage these systems in this type of network.
- Also, lack of experimentation to evaluate the performance of proposed system in its application in reality.
- Always within the limits of our work, we must know that even with optimization, coupling cryptography IDS will lead to a significant energy consumption.

Future directions

The work done during the thesis offers several prospects that are located in the extension of the work. We detail the major perspectives in what follows.

Formal verification

The validation of our formal modeling of the impact of security policies in a 6LoWPAN network is our priority at the moment. Indeed, formal verification techniques taking into account the energy are useful to analyze comprehensively the problem of energy consumption in the network. Formal verification is an essential tool for understanding the disadvantages of a given mechanism.

For example, to test a communication protocol by analyzing all possible cases is very difficult to achieve using only simulations or experiments. So it will be interesting to test the application of our proposal for the key management system on other cryptographic algorithms to study the advantage and disadvantage of an algorithm over another. First, it is necessary to find the abstractions and simplifications needed to do in order to have a functional and accurate model while maintaining the desired operating network. So have a more detailed description would be an advantage to address the real case and get more relevance on the obtained results. In addition, we need to start thinking about how these models can be applied to systems that are more complex.

Problem of securing the neighbor discovery mechanism

The neighbor monitoring security mechanism used in our work is based on the exchange of information between neighboring nodes. This exchange mechanism is used by many other approaches. The major problem with all sensors network security mechanisms is that each attack is treated alone. However, the attacker can try to execute a well-defined combination of several simultaneous attacks in the network. In this context, the challenge is to secure the exchange between the various entities of the network to ensure the validity of data. Thus, a first track would be to do statistical analysis on all the information gathered in one place and later try to correlate this with the identities of the nodes so that the number of attackers remains below a certain threshold and influence will be limited in the network.

Improvements

In addition, several perspectives can be envisaged to improve our solution:

- Adaptation of our solution with other platforms, protocols and topologies as the Internet of Things is an heterogeneous environment.
- Implement our models in a large-scale network and study the generated time, and time required to manage the cryptographic keys and detect all attacks in the network
- Implementing a machine learning system for the IDS global agent, to expand the detection area and improve the effectiveness of its prevention.
- The addition of a module for the nodes energy management, adapting a collaborative approach for the management of cryptographic keys and the management of the location of the IDS agents.
- In the end, the formal modeling of our system to deter and investigate all possibilities of threats and its experimentation in a real environment to evaluate its performance.

Conclusion

Sécuriser le secret médical au sein de l'Internet des objets basé sur les réseaux 6LoWPAN est un véritable challenge. En effet, un réseau LoWPAN en général est un environnement hostile, qui apporte plusieurs défis de sécurité, dû à ses caractéristiques et ses spécificités (réseaux ad hoc, capacités limités, contraintes de ressources, etc ...). A ces contraintes de sécurité, s'ajoutent les vulnérabilités de son intégration à l'internet, de par sa nature, un monde pourvu de plusieurs menaces sous différentes formes. Le déploiement des réseaux 6LoWPAN dans les applications de santé induit également de nouvelles épreuves à prendre en compte lors de la conception de solution au défi lié à la sécurité.

Le traitement de notre travail est scindé en cinq chapitres en dehors de l'introduction et la conclusion, dont nous avons précisé l'état de l'art en matière des applications de l'Internet des objets dans le domaine de la santé en appuyant sur le réseau 6LoWPAN après une analyse exhaustive des besoins liés à la sécurité où on a tiré les principales problématiques, sur lesquelles on s'est basé afin d'établir des solutions convenables de sécurité. Nous avons proposé deux solutions à cet effet, un système de gestion de clés comme première ligne de défense et un système de détection d'intrusion comme deuxième ligne de défense.

Résumé des chapitres

Nous avons commencé dans le **premier chapitre** par un examen des défis apportés par le passage de l'Internet traditionnel à l'Internet des objets. Nous avons intro-

duit le concept de l'internet des objets, et comment les applications d'e-santé en bénéficient. Nous avons rapporté également une introduction aux dispositifs de détection ; les capteurs sans fil, leur fonctionnement et leurs contraintes.

Nous avons expliqué que l'objectif de la création de l'internet des objets et le développement de ses mécanismes est de rendre les dispositifs plus autonomes et indépendants du contrôle direct de l'utilisateur humain, ainsi, pour lui permettre de surveiller et de contrôler à distance ces dispositifs. L'autre objectif de cette évolution est d'obtenir plus d'opportunités dans l'aide à la prise de décision. Le Gold standard de l'internet des objets est l'énorme impact qu'il aura sur plusieurs aspects de la vie et le comportement du quotidien des utilisateurs potentiels. Nous avons introduit également dans ce chapitre la technologie 6LoWPAN (IPv6 Low power Wireless Personal Area Networks); L'IPv6 sur les réseaux sans fil personnels à faible puissance. Nous avons expliqué le contexte dont l'IETF a développé la technologie 6LoWPAN afin de permettre à ces appareils de se connecter à l'Internet, et de rendre le concept de l'internet des objets une réalité.

Nous avons discuté comment l'internet des objets offrira de nombreuses opportunités intéressantes dans plusieurs domaines : surveillance industrielle et structurelle, surveillance de l'environnement, à l'automobile, l'automatisation, etc., mais nulle part il offre une plus grande promesse que dans le domaine de l'e-santé, où ses principes sont déjà appliquées pour améliorer l'accès aux soins, améliorer leur qualité et réduire leurs coûts. Les applications d'e-santé sont conçues afin d'améliorer les services de santé existants et améliorer les techniques de la surveillance à distance, surtout pour les personnes avec des difficultés tels les malades à risque, les handicapés, les personnes âgées, les enfants et les malades chroniques. L'automatisation de la collecte des données réduit le risque d'erreur humaine, les soignants dans ce cas fourniront des informations fiables sur le patient avec un taux d'erreur négligeable. Cela permettra d'améliorer la qualité du diagnostic et éviter toute erreur humaine pendant la collecte ou la transmission des informations, qui peut avoir un impact néfaste sur la santé des patients.

Nous avons traité dans le **deuxième chapitre** la technologie 6LoWPAN en déterminant ses mécanismes, les enjeux confrontés ainsi que les exigences de son appli-

cation sur le terrain. Sur ce nous avons analysé les différentes solutions qui ont été proposées pour relever ces défis.

Les réseaux 6LoWPAN sont créés en connectant des îlots de dispositifs de capteurs sans fil où chaque île présente un réseau de bout sur l'Internet. C'est un réseau que les paquets IP sont envoyés vers ou à partir de sa destination, mais qui n'agit pas comme une passerelle vers d'autres réseaux. L'architecture 6LoWPAN se compose d'un seul ou d'un ensemble de LoWPANs. Afin d'obtenir un réseau 6LoWPAN, nous devons avoir un réseau LoWPAN qui combine deux types de dispositifs de ressources limitées optant d'une adresse IPv6: hôte et routeur. Le dispositif hôte présente le point final du réseau, et le routeur agit comme un lien entre les dispositifs d'extrémité. Cette séparation des dispositifs s'établi en accord à la division proposé dans la norme IEEE 802.15.4 qui répartit les dispositifs en deux types : FFD (de l'anglais Full Function Devices, « équipement ayant la totalité des fonctions ») ou RFD (de l'anglais Reduced Function Devices, « équipement ayant des fonctions réduites »). Ces nœuds communiquent entre eux sans fil en mode ad hoc, c'est à dire sans avoir aucune infrastructure et ils partagent le même préfixe IPv6. En ce qui concerne la communication avec d'autres réseaux IP, il s'établi à travers le routeur de bordure du 6LoWPAN (6LBR). Le 6LBR est une machine puissante, chargé de déterminer le préfixe IPv6 et sa distribution aux nœuds, assume le rôle du moniteur et le contrôleur du LoWPAN, réglemente le trafic de paquets envoyés et reçus, soutient les opérations de compression de l'en-tête du paquet, gère les opérations du protocole Neighbor Discovery (découverte de voisinage), là où chaque nœud dans le LoWPAN doit s'enregistrer dans la base de données du 6LBR.

En ce qui concerne le routage, le réseau 6LoWPAN a introduit de nouveaux concepts et des mesures qui ne sont pas traités par d'autres protocoles de routage standard dans les réseaux sans fil. Un nouveau groupe de travail IETF a été créée sous le nom de ROLL (Routing Over Low power and Lossy networks) pour répondre aux exigences du routage dû à la mise en œuvre de la nouvelle couche d'adaptation (couche 6LoWPAN) dans ces réseaux. Le groupe de travail IETF-ROLL propose le protocole de routage RPL (Routing Protocol for Low power and lossy

networks) basé sur le concept du DAG (graphe orienté acyclique, de l'anglais « Direct Acyclic Graph ») pour éviter de créer des boucles dans l'arbre construit par l'algorithme de vecteur de distance. RPL a la capacité de construire multiples chemins de retour vers la même destination et définit les itinéraires de rechange lorsque les routes par défaut sont inaccessibles. Ce protocole ciblera les réseaux de ressources limitées en termes d'énergie, de puissance, de bande passante et ayant une forte probabilité de perte de paquets avec un taux d'erreur très important.

Dans le **troisième chapitre**, nous avons étudié la question sécurité dans les réseaux 6LoWPAN et nous avons fourni une analyse détaillée de tous les aspects informatiques, les objectifs, les menaces, les attaques ainsi que les solutions proposées. Dans chaque section, nous avons résumé les principales exigences auxquelles on doit faire face afin de concevoir un système de sécurité conforme aux réseaux 6LoWPAN pour les applications d'e-santé.

Nous avons expliqué que les menaces 6LoWPAN peuvent être divisées en deux catégories. Ceux qui visent à violer la confidentialité, l'authentification et l'intégrité du réseau, et ceux qui ont comme objectif de briser sa performance. Notre objectif pour assurer la sécurité est de fournir un système de cryptage qui protège les données de réseau et un système de contrôle qui cherche à détecter le comportement anormal malveillant dans le fonctionnement du réseau et l'empêcher de nuire à la performance de ce dernier. Notre principal défi dans la conception d'un système de sécurité pour le réseau 6LoWPAN était de sélectionner des techniques optimales qui doivent être adapté aux contraintes de ressources de ses appareils.

Nous avons considéré les conclusions des analyses tirées dans ce chapitre afin d'éviter les lacunes des solutions existantes. Nous avons proposé un système de détection d'intrusion qui protège les fonctionnalités et la disponibilité des réseaux 6LoWPAN et fournit simultanément la sécurité des communications internes et externes du réseau, là où la plupart des solutions existantes se concentrent seulement sur un de ces deux. Bien que notre solution soit conçue pour les applications d'e-santé, il peut être adapté à d'autres domaines.

Selon notre étude précédente, nous avons conclu que la cryptographie symétrique est la plus appropriée pour les réseaux 6LoWPAN par rapport à la cryptographie

asymétrique, car elle ne consomme pas beaucoup d'énergie, elle est rapide et la taille des clés est petite. Cependant, le problème majeur avec ce type de cryptographie est l'établissement de clés, là où en particulier les appareils des réseaux 6LoWPAN devront communiquer par Internet avec d'autres dispositifs étranges ; qui ne partagent avec eux aucune information préétablie. Nous proposons un système de gestion des clés pour la cryptographie symétrique qui fournit une solution exhaustive en sécurité et efficace en énergie.

Ainsi, en ce qui concerne le système de détection d'intrusion (IDS), nous avons établi un ensemble d'exigences qu'un IDS doit satisfaire, tels que la préservation de la puissance de transmission, ce qui minimise l'échange de données entre les nœuds, en minimisant l'impact d'une attaque possible dans les applications critiques, de fonctionner en temps réel, la surveillance des voisins, et se placer d'une manière distribuée basant sur la coopération des agents IDS. Nous avons conçu un système qui répond à ces exigences, tout en offrant un niveau élevé de détection d'intrusion et une consommation faible d'énergie.

Le **quatrième chapitre** présente notre première ligne de défense ; le système d'établissement des clés de cryptographie. Nous avons conçu ce système pour fournir une solution pour l'établissement des clés dans les réseaux 6LoWPAN pour assurer sa sécurité, en tenant compte des exigences de performance dont l'optimisation de l'énergie, l'évolutivité, la flexibilité, la mobilité et la connectivité. Notre solution offre trois types de clés de sécurité : une clé par paires entre l'unité centrale médicale MCU (Medical Center Unit) et chaque nœud sur le réseau 6LoWPAN, une clé de groupe partagé entre un nœud parent et ses nœuds enfants, et une clé de session de bout en bout entre un nœud 6LoWPAN et autre dispositif IP sur Internet. Nous fournissons également une évaluation détaillée des résultats du point de vue sécurité et consommation d'énergie qui prouve la pertinence de notre approche proposée.

Sur la base des résultats de nos expériences, nous réclamons que notre solution fournit un régime optimal pour la gestion des clés. Jusqu'à la rédaction de ce document, nous n'avons pas trouvé dans la littérature une solution de cryptographie symétrique complète qui sécurise les communications internes et externes du

réseau 6LoWPAN. La plupart des solutions sont des techniques d'adaptation créés pour les réseaux de capteurs afin assurer la sécurité à l'intérieur du 6LoWPAN et d'autres techniques légères de solutions de bout-en-bout pour assurer la sécurité des communications en dehors du 6LoWPAN. Offrant une solution à un cas indépendamment des autres peut fournir une solution efficace mais elle est incomplète pour les réseaux 6LoWPAN qui présentent une entité complète, les nœuds ont besoin de communiquer en interne avec la possibilité d'établir des communications en externe à travers l'Internet. Puisque les nœuds ont des ressources faibles, le faite de combiner plusieurs protocoles distincts avec un seul objectif, qui est la sécurité du réseau, va surcharger les nœuds et le réseau.

Le **cinquième** et le **dernier chapitre** a présenté la deuxième ligne de défense ; le système de détection d'intrusion (IDS). Nous avons proposé une nouvelle approche de détection basée sur la surveillance du comportement des nœuds voisins. C'est une nouvelle approche de détection d'intrusion qui a été récemment proposé pour l'identification des nœuds malveillants dans les réseaux avec contraintes de ressources. Elle est basée sur le fait que les nœuds voisins ont tendance à avoir le même comportement, c'est-à-dire le même nombre de paquets envoyés, reçus, et rejeté, la même force du signal généré, etc.

Nous avons proposé d'établir l'IDS sous forme d'un agent puissant global qui s'exécute au niveau de la station de base et un agent léger fonctionnant sur chaque nœud. L'agent global a accès aux informations de tous les nœuds du réseau. D'autre part, les agents locaux au niveau des nœuds surveillent leurs voisins. Son principal objectif est de détecter la mauvaise conduite des nœuds malveillants et lance une alerte à la station de base. Les résultats montrent que le système proposé est capable de résister aux attaques avec efficacité et avec moins de consommation d'énergie.

Notre problématique de recherche d'IDS dans les réseaux 6LoWPAN était dans l'utilisation des politiques de détection d'intrusion et l'emplacement de ces agents dans les nœuds du réseau. Deux grandes techniques de détection ont été proposées dans la littérature ; la détection basée sur la signature et la détection basée sur l'anomalie. Chaque technique a des avantages et des inconvénients. Notre idée

était l'utilisation des avantages de ces techniques de défense avec une limitation maximale des charges de calculs et de la communication générée par les agents IDS. Ainsi, nous avons essayé de les placer de manière optimale dans le réseau pour couvrir l'ensemble du réseau et avoir une vue globale de tous les nœuds. Ceci a conduit à la détection de tous les paquets malveillants générés par les attaquants.

Perspectives

Le travail effectué au cours de la thèse offre plusieurs perspectives qui sont situés dans le prolongement du travail. Nous détaillons seulement deux majeures perspectives dans ce qui suit.

Vérification formelle

La validation de notre modélisation formelle sur l'impact des politiques de sécurité dans un réseau 6LoWPAN est notre priorité pour le moment. En effet, les techniques de vérification formelle en tenant compte de l'énergie sont utiles pour analyser de manière exhaustive le problème de la consommation d'énergie dans le réseau. La vérification formelle est un outil essentiel pour comprendre les inconvénients d'un mécanisme donné.

Par exemple, pour tester un protocole de communication par l'analyse de tous les cas possibles est très difficile à réaliser en utilisant uniquement des simulations ou des expériences. Ainsi, il sera intéressant de tester l'application de notre proposition du système de gestion de clés sur d'autres algorithmes cryptographiques pour étudier l'avantage et le désavantage d'un algorithme par rapport un autre. Mais d'abord, il est nécessaire de trouver les abstractions et les simplifications nécessaires à faire afin d'avoir un modèle fonctionnel et précis tout en maintenant le fonctionnement souhaité d'un réseau 6LoWPAN. Donc, avoir une description plus détaillée serait un avantage pour aborder le cas réel et d'obtenir plus de pertinence sur les résultats obtenus. En outre, nous devons commencer à penser sur comment ces modèles peuvent être appliqués sur des systèmes plus compliqués.

Problème d'assurer le mécanisme de découverte de voisinage

Le mécanisme de sécurité de voisinage utilisé dans notre travail est basé sur l'échange d'informations entre les nœuds voisins. Ce mécanisme d'échange est utilisé par de nombreuses autres approches. Le problème majeur avec tous les mécanismes de sécurité de réseau de capteurs est que chaque attaque est traitée seule. Cependant, l'attaquant peut essayer d'exécuter une combinaison bien définie de plusieurs attaques simultanément dans le réseau. Dans ce contexte, le défi est de sécuriser les échanges entre les différentes entités du réseau afin d'assurer la validité des données. Ainsi, une première piste serait de faire des analyses statistiques sur toutes les informations recueillies dans un endroit et essayez plus tard de corréler tout cela avec les identités des nœuds de sorte que le nombre d'attaquants reste en dessous d'un certain seuil et leur influence soit limitée dans le réseau.

Améliorations

Par ailleurs, plusieurs perspectives peuvent être envisagées pour améliorer davantage ces travaux:

- L'adaptation du fonctionnement de notre solution avec les autres plateformes, protocoles et topologies du faite que l'IdO est un environnement hétérogène
- Implémenter nos modèles dans un réseau à grande échelle et étudier le délai généré, et le temps requis, pour gérer les clés de cryptographie et détecter toutes les attaques survenues dans le réseau
- L'implémentation d'un système d'apprentissage automatique pour l'agent global du système IDS, afin d'élargir le champ de détection, et d'améliorer l'efficacité de ses préventions.
- L'ajout d'un module appart pour la gestion de l'énergie des nœuds, en adaptant une approche collaborative pour la gestion des clés de cryptographie et la gestion de l'emplacement des agents IDS.

- En fin, la modélisation formelle de notre système pour contrecarrer et étudier toutes les possibilités de menaces, et son expérimentation dans un environnement réel pour évaluer ses performances.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] "Internet of Things (IoT) Opportunities," Cisco. [Online]. Available: http://www.cisco.com/web/solutions/trends/iot/indepth.html.

[3] "When everything connects," The Economist, Apr-2007.

[4] D. Minoli, "Internet of Things Application Examples," in Building the Internet of Things with IPv6 and MIPv6, John Wiley & Sons, Inc., 2013, pp. 48–96.

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[6] Xiaojun Wang, Riji Yu, Feng Liu, Shushan Hu, and Cunchen Tang, "Connected intelligent home based on the Internet of things," 2013, pp. 41–45.

[7] L. Tan and N. Wang, "Future internet: The Internet of Things," in 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010, vol. 5, pp. V5–376–V5–380.

[8] "ITU releases latest tech figures and global rankings." [Online]. Available: http://www.itu.int/net/pressoffice/press_releases/2013/41.aspx.

[9] T. Zahariadis, D. Papadimitriou, H. Tschofenig, S. Haller, P. Daras, G. D. Stamoulis, and M. Hauswirth, "Towards a Future Internet Architecture," in The Future Internet, Eds. Springer Berlin Heidelberg, 2011, pp. 7–18.

[10] "That 'Internet of Things' Thing - RFID Journal." [Online]. Available: http://www.rfidjournal.com/articles/view?4986.

[11] "Internet of Things 2008 Conference, March 26-28, Zurich." [Online]. Available: http://www.the-internet-of-things.org/iot2008/.

[12] "IPSO Alliance | Enabling the Internet of Things." [Online]. Available: http://www.ipso-alliance.org/.

[13] "Institute of Electrical and Electronics Engineers." [Online]. Available: https://www.ieee.org/.

[14] "P2413 WG." [Online]. Available: http://grouper.ieee.org/groups/2413/.

[15] "IEEE Standards Group Wants to Bring Order to IoT." [Online]. Available: http://cacm.acm.org/news/178795-ieee-standards-group-wants-to-bring-order-to-iot/fulltext.

[16] "ETSI - Standards for an Internet of Things: A workshop," ETSI. [Online]. Available: http://www.etsi.org/news-events/events/771-2014-etsi-ec-dg-connect-iot.

[17] "ISO/IEC NP 19654 - Internet of Things Reference Architecture (IoT RA)." [Online]. Available: http://www.iso.org/

[18] J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, and D. Boyle, "The Vision for Moving from M2M to IoT," in From Machine-To-Machine to the Internet of Things, Eds. Oxford: Academic Press, 2014, p. 1.

[19] "Gartner's 2012 Hype Cycle for Emerging Technologies Identifies." [Online]. Available: http://www.gartner.com/newsroom/id/2124315.

[20] J. Postel, "Internet Protocol." [Online]. Available: https://tools.ietf.org/html/rfc791.

[21] W. Fan and Y. Li, "Opportunities, Challenges and Practices of the Internet of Things," 10-May-2010. [Online]. Available: http://wwwen.zte.com.cn/

[22] "Internet Engineering Task Force (IETF)." [Online]. Available: https://www.ietf.org/.

[23] "6lowpan WG - IPv6 over low power WPAN." [Online]. Available: https://tools.ietf.org/wg/6lowpan/.

[24] Edmonson, B. Wakefield, and A. E. Lancaster, "Care Coordination/Home Telehealth: The Systematic Implementation of Health Informatics, Home Telehealth, and Disease Management to Support the Care of Veteran Patients with Chronic Conditions," Telemed. E-Health, vol. 14, no. 10, pp. 1118–1126, Dec. 2008.

[25] S. Sneha and U. Varshney, "Enabling ubiquitous patient monitoring: Model, decision protocols, opportunities and challenges," Decis. Support Syst., vol. 46, no. 3, pp. 606–619, Feb. 2009.

[26] A. Dewabharata, D. M.-H. Wen, and S.-Y. Chou, "An Activity Ontology for Context-Aware Health Promotion Application," in Computer Software and Applications Conference Workshops (COMPSACW), 2013 IEEE 37th Annual, 2013, pp. 421–426.

[27] "Chairman Proposal To Spur Innovation In Medical Body Area Networks." [Online]. Available: http://www.fcc.gov/document/chairman-proposal-spur-innovation-medical-body-area-networks.

[28] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," Comput. Netw., vol. 54, no. 15, pp. 2688–2710, Oct. 2010.

[29] F. Schelfhout and J. Meeus, "do I need IoT in Healthcare?," Domestic sensor networks. .

[30] Z. Pang, L. Zheng, J. Tian, S. Kao-Walter, E. Dubrova, and Q. Chen, "Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things," Enterp. Inf. Syst., vol. 0, no. 0, pp. 1–31, Apr. 2013.

[31] A. J. Jara, M. A. Zamora-Izquierdo, and A. F. Skarmeta, "Interconnection Framework for mHealth and Remote Monitoring Based on the Internet of Things," IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 47–65, Sep. 2013.

[32] American Heart Association Statistics Committee and Stroke Statistics Subcommittee, "Heart disease and stroke statistics–2013 update: a report from the American Heart Association," Circulation, vol. 127, no. 1, pp. e6–e245, Jan. 2013.

[33] M. Rosu and S. Pasca, "A WBAN-ECG approach for real-time long-term monitoring," in 2013 8th International Symposium on Advanced Topics in Electrical Engineering (ATEE), 2013, pp. 1–6.

[34] N. Bui and M. Zorzi, "Health Care Applications: A Solution Based on the Internet of Things," in Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, New York, NY, USA, 2011, pp. 131:1–131:5.

[35] C. Wang, Q. Wang, and S. Shi, "A distributed wireless body area network for medical supervision," in Instrumentation and Measurement Technology Conference (I2MTC), 2012 IEEE International, 2012, pp. 2612–2616.

[36] "Wireless body area network." [Online]. Available: http://www2.imse-cnm.csic.es/ mandel/wban.htm.

[37] A. Burns, B. R. Greene, M. J. McGrath, T. J. O'Shea, B. Kuris, S. M. Ayer, F. Stroiescu, and V. Cionca, "SHIMMER. A Wireless Sensor Platform for Non-invasive Biomedical Research," IEEE Sens. J., vol. 10, no. 9, pp. 1527–1534, Sep. 2010.

[38] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, "IEEE 802.15.4: a developing standard for low-power low-cost wireless personal area networks," IEEE Netw., vol. 15, no. 5, pp. 12–19, Sep. 2001.

[39] "Berkeley TelosB Mote." [Online]. Available: http://www.eecs.berkeley.edu/cūller/WEI/labs/lab1-IP/Lab01.html.

[40] G. Asch, Les capteurs en instrumentation industrielle. Paris: Dunod, 1993.

[41] S. Middelhoek and A. C. Hoogerwerf, "Smart sensors: when and where?," Sens. Actuators, vol. 8, no. 1, pp. 39–48, Sep. 1985.

[42] "TinyOS." [Online]. Available: http://www.tinyos.net/.

[43] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Comput. Netw., vol. 52, no. 12, pp. 2292–2330, Aug. 2008.

[44] D. Feng, C. Jiang, G. Lim, J., L.J. Cimini, G. Feng, and G. Y. Li, "A survey of energy-efficient wireless communications," IEEE Commun. Surv. Tutor., vol. 15, no. 1, pp. 167–178, First 2013.

[45] K. Beydoun, V. Felea, and H. Guyennet, "Wireless Sensor Network Infrastructure: Construction and Evaluation," in Fifth International Conference on Wireless and Mobile Communications, 2009. ICWMC '09, 2009, pp. 279–284.

[46] Z. Shelby and C. Bormann, 6LoWPAN: The Wireless Embedded Internet. Wiley, 2009.

[47] S. E. Deering, "Internet Protocol, Version 6 (IPv6) Specification." [Online]. Available: https://tools.ietf.org/html/rfc2460.

[48] "Internet Assigned Numbers Authority." [Online]. Available: http://www.internetassignednumbersauthority.com/.

[49] "Free Pool of IPv4 Address Space Depleted | The Number Resource Organization." .

[50] C. P. P. Schumacher, N. Kushalnagar, and G. Montenegro, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals." [Online]. Available: https://tools.ietf.org/html/rfc4919.

[51] N. Kushalnagar, G. Montenegro, D. E. Culler, and J. W. Hui, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks." [Online]. Available: http://tools.ietf.org/html/rfc4944.

[52] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks." [Online]. Available: https://tools.ietf.org/html/rfc6282.

[53] S. Chakrabarti, Z. Shelby, and E. Nordmark, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)." [Online]. Available: http://tools.ietf.org/html/rfc6775.

[54] T. Narten, W. A. Simpson, E. Nordmark, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)." [Online]. Available: https://tools.ietf.org/html/rfc4861.

[55] K.-H. Kim, W. Haddad, J. Laganier, S. Park, and S. Chakrabarti, "IPv6 over Low Power WPAN Security Analysis." [Online]. Available: https://tools.ietf.org/html/draft-daniel-6lowpan-security-analysis-05.

[56] R. K. Alexander, M. Richardson, T. Tsao, V. Daza, A. Lozano, and M. Dohler, "A Security Threat Analysis for Routing Protocol for Low-power and lossy networks (RPL)." [Online]. Available: http://tools.ietf.org/html/draft-ietf-roll-security-threats-07.

[57] K. Sohraby, D. Minoli, and Z. Taieb, Wiley: Wireless Sensor Networks: Technology, Protocols, and Applications. John Wiley and Sons, 2007.

[58] "6lo WG - IPv6 over Networks of Resource-constrained Nodes." [Online]. Available: https://tools.ietf.org/wg/6lo/.

[59] L. Kerry, J. Martocci, C. Neilson, and S. Donaldson, "draft-ietf-6man-6lobac-01," 2012. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-6man-6lobac/.

[60] P. Mariager, J. Peterson, and Z. Shelby, "draft-mariager-6lowpan-v6over-dect-ule-03," 2014. [Online]. Available: https://datatracker.ietf.org/doc/draft-mariager-6lowpan-v6over-dect-ule/.

[61] C. Bormann, "draft-bormann-6lo-6lowpan-roadmap-00," 2014. [Online]. Available: https://datatracker.ietf.org/doc/draft-bormann-6lo-6lowpan-roadmap/.

[62] C. Bormann, "draft-bormann-6lo-ghc-00," 2013. [Online]. Available: https://datatracker.ietf.org/doc/draft-bormann-6lo-ghc/.

[63] J. Schönwälder, A. Sehgal, T. Tsou, and C. Zhou, "draft-schoenw-6lo-lowpan-mib-01," 2013. [Online]. Available: https://datatracker.ietf.org/doc/draft-schoenw-6lo-lowpan-mib/.

[64] A. Brandt and J. Buron, "draft-brandt-6man-lowpanz-02," 2013. [Online]. Available: https://datatracker.ietf.org/doc/draft-brandt-6man-lowpanz/.

[65] P. Thubert and J. Hui, "draft-thubert-6lo-forwarding-fragments-01," 2014. [Online]. Available: https://datatracker.ietf.org/doc/draft-thubert-6lo-forwarding-fragments/.

[66] D. Popa and J. W. Hui, "6LoPLC: Transmission of IPv6 Packets over IEEE 1901.2 Narrowband Powerline Communication Networks," 2014. [Online]. Available: http://tools.ietf.org/html/draft-popa-6lo-6loplc-ipv6-over-ieee19012-networks-00.

[67] G. Rizzo, A. Jara, A. Olivieri, and Y. Bocchi, "draft-rizzo-6lo-6legacy-02," 2014. [Online]. Available: https://datatracker.ietf.org/doc/draft-rizzo-6lo-6legacy/.

[68] R. M. Hinden and B. Haberman, "Unique Local IPv6 Unicast Addresses." [Online]. Available: https://tools.ietf.org/html/rfc4193.

[69] R. Braden, "Requirements for Internet Hosts - Communication Layers." [Online]. Available: https://tools.ietf.org/html/rfc1122.

[70] "Guidelines for 64-bit global identifier (EUI-64 TM) registration authority." [Online]. Available: http://grouper.ieee.org/groups/msc/MSCRacInfo/EUI64.htm.

[71] N. Halimatul, A. Ismail, and K. W. M. Ghazali, "A Study on Protocol Stack in 6lowpan Model". Journal of Theoretical and Applied Information Technology, 41 (2). pp. 220-229, 2012.

[72] J. Schaad and R. Housley, "Advanced Encryption Standard (AES) Key Wrap Algorithm." [Online]. Available: https://tools.ietf.org/html/rfc3394.

[73] J. Postel, "User Datagram Protocol." [Online]. Available: https://tools.ietf.org/html/rfc768.

[74] J. Postel, "Internet Control Message Protocol." [Online]. Available: https://tools.ietf.org/html/rfc792.

[75] J. Postel, "Transmission Control Protocol." [Online]. Available: https://tools.ietf.org/html/rfc793.

[76] P. J. Leach, T. Berners-Lee, J. C. Mogul, L. Masinter, R. T. Fielding, and J. Gettys, "Hypertext Transfer Protocol – HTTP/1.1." [Online]. Available: https://tools.ietf.org/html/rfc2616.

[77] J. Postel and J. Reynolds, "File Transfer Protocol." [Online]. Available: https://tools.ietf.org/html/rfc959.

[78] E. Schooler, G. Camarillo, M. Handley, J. Peterson, J. Rosenberg, A. Johnston, H. Schulzrinne, and R. Sparks, "SIP: Session Initiation Protocol." [Online]. Available: https://tools.ietf.org/html/rfc3261.

[79] V. Jacobson, R. Frederick, S. Casner, and H. Schulzrinne, "RTP: A Transport Protocol for Real-Time Applications." [Online]. Available: https://tools.ietf.org/html/rfc3550.

[80] E. Guttman and J. Veizades, "Service Location Protocol, Version 2." [Online]. Available: https://tools.ietf.org/html/rfc2608.

[81] J. Davin, J. D. Case, M. Fedor, and M. L. Schoffstall, "Simple Network Management Protocol (SNMP)." [Online]. Available: https://tools.ietf.org/html/rfc1157.

[82] "IEEE-SA - OUI (Organizationally Unique Identifier)." [Online]. Available: http://standards.ieee.org/develop/regauth/oui/.

[83] R. Droms and O. Troan, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6." [Online]. Available: https://tools.ietf.org/html/rfc3633.

[84] T. Savolainen, S. Krishnan, O. Troan, and J. Korhonen, "Prefix Exclude Option for DHCPv6-based Prefix Delegation." [Online]. Available: https://tools.ietf.org/html/rfc6603.

[85] S. Miyakawa and R. Droms, "Requirements for IPv6 Prefix Delegation." [Online]. Available: https://tools.ietf.org/html/rfc3769.

[86] T. Narten, S. Thomson, and T. Jinmei, "IPv6 Stateless Address Autoconfiguration." [Online]. Available: http://tools.ietf.org/html/rfc4862.

[87] A. Conta and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification." [Online]. Available: https://tools.ietf.org/html/rfc4443.

[88] N. Moore, "Optimistic Duplicate Address Detection (DAD) for IPv6." [Online]. Available: https://tools.ietf.org/html/rfc4429.

[89] J. Arkko, D. B. Johnson, and C. E. Perkins, "Mobility Support in IPv6." [Online]. Available: https://tools.ietf.org/html/rfc3775.

[90] V. Devarapalli, K. Chowdhury, S. Gundavelli, B. Patil, and K. Leung, "Proxy Mobile IPv6." [Online]. Available: https://tools.ietf.org/html/rfc5213.

[91] A. Petrescu, R. Wakikawa, P. Thubert, and V. Devarapalli, "Network Mobility (NEMO) Basic Support Protocol." [Online]. Available: https://tools.ietf.org/html/rfc3963.

[92] J. H. Kim, C. S. Hong, and T. Shon, "A Lightweight NEMO Protocol to Support 6LoWPAN," ETRI J., vol. 30, no. 5, pp. 685–695, 2008.

[93] G. Bag, H. Mukhtar, S. M. S. Shams, K. H. Kim, and S. Yoo, "Inter-PAN Mobility Support for 6LoWPAN," in Third International Conference on Convergence and Hybrid Information Technology, 2008. ICCIT '08, 2008, vol. 1, pp. 787–792.

[94] Z. Zinonos and V. Vassiliou, "Inter-mobility support in controlled 6LoWPAN networks," in 2010 IEEE GLOBECOM Workshops (GC Wkshps), 2010, pp. 1718–1723.

[95] M. Ha, D. Kim, S. H. Kim, and S. Hong, "Inter-MARIO: A Fast and Seamless Mobility Protocol to Support Inter-Pan Handover in 6LoWPAN," in 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010), 2010, pp. 1–6.

[96] M. M. Islam and E.-N. Huh, "Sensor Proxy Mobile IPv6 (SPMIPv6)—A Novel Scheme for Mobility Supported IP-WSNs," Sensors, vol. 11, no. 2, pp. 1865–1887, Feb. 2011.

[97] S. R. Das, E. M. Belding-Royer, and C. E. Perkins, "Ad hoc On-Demand Distance Vector (AODV) Routing." [Online]. Available: https://tools.ietf.org/html/rfc3561.

[98] P. Jaquet, "Optimized Link State Routing Protocol (OLSR)." [Online]. Available: https://tools.ietf.org/html/rfc3626.

[99] S. Ratliff, J. Dowdell, and C. Perkins, "Dynamic MANET On-demand (AODVv2) Routing." [Online]. Available: https://tools.ietf.org/html/draft-ietf-manet-dymo-26.

[100] D. A. Maltz and D. B. Johnson, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4." [Online]. Available: https://tools.ietf.org/html/rfc4728.

[101] M. Felsche, A. Huhn, and H. Schwetlick, "Routing Protocols for 6LoWPAN," in IT Revolutions, M. L. Reyes, J. M. F. Arias, J. J. G. de la Rosa, J. Langer, F. J. B. Outeiriño, and A. Moreno-Munñoz, Eds. Springer Berlin Heidelberg, 2012, pp. 71–83.

[102] V. Kumar and S. Tiwari, "Routing in IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): A Survey," J. Comput. Netw. Commun., vol. 2012, p. e316839, Mar. 2012.

[103] J. Martocci, P. Mil, N. Riou, and W. Vermeylen, "Building Automation Routing Requirements in Low-Power and Lossy Networks." [Online]. Available: https://tools.ietf.org/html/rfc5867.

[104] M. Dohler, D. Barthel, T. Watteyne, and T. Winter, "Routing Requirements for Urban Low-Power and Lossy Networks." [Online]. Available: http://tools.ietf.org/html/rfc5548.

[105] T. Winter, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks." [Online]. Available: https://tools.ietf.org/html/rfc6550.

[106] M. Nottingham and M. A. Baker, "The 'application/soap+xml' media type." [Online]. Available: http://tools.ietf.org/html/rfc3902.

[107] P. Francis and K. Egevang, "The IP Network Address Translator (NAT)." [Online]. Available: http://tools.ietf.org/html/rfc1631.

[108] E. Rescorla and B. Korver, "Guidelines for Writing RFC Text on Security Considerations." [Online]. Available: http://tools.ietf.org/html/rfc3552.

[109] A. Liu, M. Kim, L. B. Oliveira, and H. Tan, "Wireless Sensor Network Security," Int. J. Distrib. Sens. Netw., vol. 2013, p. e362385, Jan. 2013.

[110] E. Shi and A. Perrig, "Designing secure sensor networks," IEEE Wirel. Commun., vol. 11, no. 6, pp. 38–43, Dec. 2004.

[111] J. Kempf, E. Nordmark, and P. Nikander, "IPv6 Neighbor Discovery (ND) Trust Models and Threats." [Online]. Available: http://tools.ietf.org/html/rfc3756.

[112] E. J. Cho, J. H. Kim, and C. S. Hong, "Attack Model and Detection Scheme for Botnet on 6LoWPAN," in Proceedings of the 12th Asia-Pacific Network Operations and Management Conference on Management Enabling the Future Internet for Changing Business and New Computing Services, Berlin, Heidelberg, 2009, pp. 515–518.

[113] A. Freier, P. Karlton, and P. Kocher, "The Secure Sockets Layer (SSL) Protocol Version 3.0." [Online]. Available: http://tools.ietf.org/html/rfc6101.

[114] J. Jonsson and B. Kaliski, "Public-Key Cryptography Standards (PKCS) 1: RSA Cryptography Specifications Version 2.1." [Online]. Available: http://tools.ietf.org/html/rfc3447.

[115] S. G. Kelly, "Security Implications of Using the Data Encryption Standard (DES)." [Online]. Available: https://tools.ietf.org/html/rfc4772.

[116] R. W. Shirey, "Internet Security Glossary, Version 2-page-37." [Online]. Available: http://tools.ietf.org/html/rfc4949.

[117] E. Rescorla, "Diffie-Hellman Key Agreement Method," May 1999.

[118] S. Heinrich, "Public Key Infrastructure based on Authentication of Media Attestments," ArXiv13117182 Cs, Nov. 2013.

[119] D. Cooper, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." [Online]. Available: http://tools.ietf.org/html/rfc5280.

[120] R. Blom, "An Optimal Class of Symmetric Key Generation Systems," in Advances in Cryptology, T. Beth, N. Cot, and I. Ingemarsson, Eds. Springer Berlin Heidelberg, 1985, pp. 335–338.

[121] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in 3rd IEEE Consumer Communications and Networking Conference, CCNC 2006, vol. 1, pp. 640–644.

[122] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized Intrusion Detection in Wireless Sensor Networks," in Proceedings of the 1st ACM International Workshop on Quality of Service; Security in Wireless and Mobile Networks, New York, NY, USA, 2005, pp. 16–23.

[123] A. Stetsko and V. Matyas, "Effectiveness Metrics for Intrusion Detection in Wireless Sensor Networks," in 2009 European Conference on Computer Network Defense (EC2ND), 2009, pp. 21–28.

[124] F. Anjum, D. Subhadrabandhu, S. Sarkar, and R. Shetty, "On optimal placement of intrusion detection modules in sensor networks," in First International Conference on Broadband Networks, 2004. BroadNets 2004. Proceedings, 2004, pp. 690–699.

[125] P. Techateerawat and A. Jennings, "Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks," in 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology Workshops, 2006. WI-IAT 2006 Workshops, 2006, pp. 227–230.

[126] X. Wang and H. Qian, "Hierarchical and Low-power IPv6 Address Configuration for Wireless Sensor Networks," Int J Commun Syst, vol. 25, no. 12, pp. 1513–1529, Dec. 2012.

[127] K. Seo and S. Kent, "Security Architecture for the Internet Protocol." [Online]. Available: http://tools.ietf.org/html/rfc4301.

[128] D. Carrel and D. Harkins, "The Internet Key Exchange (IKE)." [Online]. Available: http://tools.ietf.org/html/rfc2409.

[129] P. Eronen, C. Kaufman, Y. Nir, and P. Hoffman, "Internet Key Exchange Protocol Version 2 (IKEv2)." [Online]. Available: http://tools.ietf.org/html/rfc5996.

[130] S. Kent, "IP Authentication Header." [Online]. Available: http://tools.ietf.org/html/rfc4302.

[131] S. Kent, "IP Encapsulating Security Payload (ESP)." [Online]. Available: http://tools.ietf.org/html/rfc4303.

[132] J. H. Saltzer, D. P. Reed, and D. D. Clark, "End-to-end Arguments in System Design," ACM Trans Comput Syst, vol. 2, no. 4, pp. 277–288, Nov. 1984.

[133] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," in 2013 9th International Conference on Computational Intelligence and Security (CIS), 2013, pp. 663–667.

[134] S. Ould Amara, R. Beghdad, and M. Oussalah, "Securing Wireless Sensor Networks: A Survey," EDPACS, vol. 47, no. 2, pp. 6–29, Feb. 2013.

[135] P. Varadarajan and G. Crosby, "Implementing IPsec in Wireless Sensor Networks," in 2014 6th International Conference on New Technologies, Mobility and Security (NTMS), 2014, pp. 1–5.

[136] Y. B. Saied, "Collaborative security for the internet of things," PhD Thesis, Institut National des Télécommunications, 2013.

[137] X. He, M. Niedermeier, and H. de Meer, "Dynamic key management in wireless sensor networks: A survey," J. Netw. Comput. Appl., vol. 36, no. 2, pp. 611–622, Mar. 2013.

[138] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in IEEE Symposium on Security and Privacy, Berkeley, California, May 11-14 2003, pp. 197–213.

[139] D. Liu and P. Ning, "Location-based pairwise key establishments for static sensor networks," in Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (CCS '03), pp. 72–82, October 2003.

[140] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in Proceedings of IEEE INFOCOM'04. 2004.

[141] S. Schmidt, H. Krahn, S. Fischer, D. Watjen, "A security architecture for mobile wireless sensor networks," in Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS'04) (Heidelberg, Germany), Vol. 3313, August 2004.

[142] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "Spins: Security protocols for sensor networks," in Proceedings of the 7th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom), Rome, Italy, July 2001, pp. 189–199.

[143] J. Lopez, "Unleashing public-key cryptography in wireless sensor networks," Journal of Computer Security, vol. 14, no. 5, pp. 469–482, 2006.

[144] N. Koblitz, "Elliptic Curve Cryptosystems," Math. Comput., vol. 48, no. 177, p. 203, Jan. 1987.

[145] N. R. Potlapally, S. Ravi, A. Raghunathan, N.K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols", IEEE Transactions on Mobile Computing, 128–143, 2006.

[146] D. J. Malan, M. Welsh, M. D. Smith, "A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography," First IEEE International Conference on Sensor and Ad Hoc Communications and Networks, 2004.

[147] P. K. Dutta, J. W. Hui, D. C. Chu, and D. E. Culler, Securing the deluge network programming system, in Proceedings of the 5th International Conference on Information Processing in Sensor Networks (IPSN). ACM, New York, NY, 326–333. 2006.

[148] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, P. Kruss, TinyPK: Securing sensor networks with public key technology, in Proceedings of the 2nd ACM workshop on Security of Ad Hoc and Sensor Networks, pp. 59–64, 2004, USA.

[149] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks," in Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications, ACM Press, 2003; 141–150.

[150] P. Kotzanikolaou, E. Magkos, D. Vergados, and M. Stefanidakis, "Secure and practical key establishment for distributed sensor networks," in Security and Communication Networks, Wiley InterScience, 2009.

[151] W. Hu, P. Corke , W. C. Shih, L. Overs, secFleck: A Public Key Technology Platform for Wireless Sensor Networks, in Proceedings of the 6th European Conference on Wireless Sensor Networks, February 11-13, 2009, Cork, Ireland.

[152] G. Gaubatz, J. Kaps, and B. Sunar, "Public key cryptography in sensor networks–revisited," Lecture Notes in Computer Science, vol. 3313, pp. 2–18, 2005.

[153] G. Gaubatz, J. Kaps, E. Ozturk, and B. Sunar, "State of the art in ultralow power public key cryptography for wireless sensor networks," in Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops. IEEE Computer Society Washington, DC, USA, 2005, pp. 146–150.

[154] J. Mache, C.-Y. Wan, and M. Yarvis, "Exploiting heterogeneity for sensor network security," in Proceedings of IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp. 591–593, 2008.

[155] R. Riaz, A. Naureen, A. Akram, A. Akbar, K. Kim, and H. Farooq Ahmed, "A unified security framework with three key management schemes for wireless sensor networks," Computer Communications, vol. 31, no. 18, pp. 4269–4280, 2008.

[156] T. D. <tim@dierks.org>, "The Transport Layer Security (TLS) Protocol Version 1.2." [Online]. Available: http://tools.ietf.org/html/rfc5246.

[157] T. Henderson, P. Jokela, P. Nikander, and R. Moskowitz, "Host Identity Protocol." [Online]. Available: https://tools.ietf.org/html/rfc5201.

[158] M. Ray, N. Oskov, S. Dispensa, and E. Rescorla, "Transport Layer Security (TLS) Renegotiation Indication Extension." [Online]. Available: https://tools.ietf.org/html/rfc5746.

[159] P. Eronen H. Tschofenig,"Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", IETF RFC 4279, December 2005.

[160] V. Gupta , M. Millard , S. Fung , Y. Zhu , N. Gura , H. Eberle , S. Chang, S. Sizzle, "A Standards-Based End-to-End Security Architecture for the Embedded Internet", Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, p.247-256, March 08-12, 2005.

[161] ANSI X9.62. "Elliptic Curve Key Agreement and Key Transport Protocols". American Bankers Association,1999.

[162] ANSI X9.63. "The Elliptic Curve Digital Signature Algorithm". American Bankers Association, 1999.

[163] W. Jung & al, "SSL-based Lightweight Security of IP-based Wireless Sensor Networks", International Conference on Advanced Information Networking and Applications Workshop (2009).

[164] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig, "Securing Communication in 6LoWPAN with Compressed IPsec", In Proceedings of the 7th IEEE International Conference on Distributed Computing in Sensor Systems (IEEE DCOSS 2011), Barcelona, Spain, June 2011.

[165] V. Nagalakshmi, I. Rameshbabu and P.S. Avadhani," Modified protocols for internet key exchange (IKE) using public encryption key and signature keys. Proc. of the eighth international conference on Information Technology: New Generations 2011; 376-381.

[166] R. Sangram, G. P. Biswas, "Establishment of ECC-based Initial Secrecy Usable for IKE Implementation", in Lecture Notes in Engineering and Computer Science, pages 530-535, 2012.

[167] T. Aura, Cryptographically Generated Addresses (CGA), IETF RFC 3972, March 2005.

[168] R. Moskowitz, HIP Diet EXchange (DEX), draft-moskowitz-hip-rg-dex-05 (IETF work in progress), March 2011.

[169] T. Heer, LHIP Lightweight Authentication Extension for HIP, draft-heer-hip-lhip-00 (IETF work in progress), February 2007.

[170] N. R. Potlapally, S. Ravi, A. Raghunathan, N.K. Jha, A study of the energy consumption characteristics of cryptographic algorithms and security protocols, IEEE Transactions on Mobile Computing, 128–143, 2006.

[171] A. Liu and P. Ning. TinyECC: A configurable library for Elliptic Curve Cryptography in Wireless Sensor Networks. Technical Report TR-2007-36, North Carolina State University, Department of Computer Science, 2007.

[172] G. De Meulenaer, F.Gosset , F.-X. Standaert, and O. Pereira, On the energy cost of communication and cryptography in wireless sensor networks, Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB 2008).

[173] A. Rghioui, M. Bouhorma, A. Benslimane. "Analytical study of security aspects in 6LoWPAN networks," In : Information and Communication Technology for the Muslim World (ICT4M), 2013 5th International Conference on. IEEE 2013, p.1-5.

[174] A. Rghioui, A. L'aarje, F. Elouaai, M. Bouhorma. "Protecting e-healthcare data privacy for Internet of Things based Wireless Body Area Network," Research Journal of Applied Sciences, Engineering and Technology, 2015, vol. 9, no. 6, p.876-885.

[175] A. Rghioui, R. Abdmeziem, S. Bouchkaren, M. Bouhorma. "Symmetric cryptography keys management for 6loWPAN networks,". Journal of Theoretical and Applied Information Technology, 2015, vol. 73, no 3, p.336-345.

[176] J. Schwartz, "U.S. Selects a New Encryption Technique," The New York Times, 03-Oct-2000.

[177] G. de Meulenaer, F. Gosset, O.-X. Standaert, and O. Pereira, "On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks," in Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and Mobile Computing, 2008, pp. 580–585.

[178] J. Lee, K. Kapitanova, and S. H. Son, "The Price of Security in Wireless Sensor Networks," Comput Netw, vol. 54, no. 17, pp. 2967–2978, Dec. 2010.

[179] K. Veress and M. Maroti, "LinkBench: Benchmark and metric framework for wireless sensor networks," in 2011 10th International Conference on Information Processing in Sensor Networks (IPSN), 2011, pp. 171–172.

[180] M. Mana, M. Feham, and B. A. Bensaber, "Trust key management scheme for wireless body area networks," Int. J. Netw. Secur.

[181] R. Abdmeziem and D. Tandjaoui, "A Lightweight Key Management Scheme for E-health applications in the context of Internet of Things," CERIST, Technical Report CERIST-DTISI/RR–14-0000000010–dz, Mar. 2014.

[182] Y. B. Saied, "Collaborative security for the internet of things," phdthesis, Institut National des Télécommunications, 2013.

[183] A. Armando & al, "The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications," in Etessami, K., Rajamani, S.K. (eds.) CAV 2005. LNCS, vol. 3576, Springer, Heidelberg (2005), http://www.avispa-project.org

[184] Y. Glouche and T. Genet. "SPAN – a Security Protocol ANimator for AVISPA – User Manual," IRISA / Université de Rennes 1, 2006. 20 pages. http ://www.irisa.fr/lande/genet/span/

[185] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach," Int. J. Commun. Syst., vol. 25, no. 9, pp. 1189–1212, Sep. 2012.

[186] J. P. Amaral, L. M. Oliveira, J. J. P. C. Rodrigues, G. Han, and L. Shu, "Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks," in 2014 IEEE International Conference on Communications (ICC), 2014, pp. 1796–1801.

[187] I. Butun, S. D. Morgera, and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," IEEE Commun. Surv. Tutor., vol. 16, no. 1, pp. 266–282, 2014.

[188] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion Detection Systems in Wireless Sensor Networks: A Review," Int. J. Distrib. Sens. Netw., vol. 2013, p. e167575, May 2013.

[189] Y. Mao ."A semantic-based intrusion detection framework for wireless sensor network". 2010 6th International Conference on Networked Computing (INC), Gyeongju, Korea (South), 2010; 1–5.

[190] R. C. Chen, Y. F. Haung, C. F. Hsieh. "Ranger intrusion detection system for wireless sensor network with sybil attack based on ontology". Third WSEAS International Conference on Biomedical Electronics and Biomedical Informatics (BEBI '10), Taipei Taiwan, 2010; 176–180.

[191] S. J. Lee, H.Y. Lee, T.H. Cho. "A threshold determining method for the dynamic filtering in wireless sensor networks based on fuzzy logic". IJCSNS International Journal of Computer Science and Network Security 2008; 8(4):155–159.

[192] S. H. Chi, T. H. Cho. "Fuzzy Logic Anomaly Detection Scheme for Directed Diffusion Based Sensor Networks". FSKD 2006, Xian, China, 2006; 725–734.

[193] B. Parekh, H. Cam. "Minimizing false alarms on intrusion detection for wireless sensor networks in realistic environments". Military Communications Conference, Orlando, Florida, 2007; 1–7.

[194] R. S. Dong, LL Liu, JM. Liu, XL. Xu. "Intrusion detection system based on payoff matrix for wireless sensor networks". Genetic and Evolutionary Computing, Guilin China, 2009; 3–6.

[195] M. Estiri, A. Khademzadeh. "A game-theoretical model for intrusion detection in wireless sensor networks". 2010 23rd Canadian Conference on Electrical and Computer Engineering (CCECE), Calgary, AB, 2010; 1–5.

[196] M. Estiri, A. Khademzadeh. "A theoretical signaling game model for intrusion detection in wireless sensor networks". 2010 14th International Telecommunications Network Strategy and Planning Symposium (NETWORKS), Warsaw, 2010; 1–6.

[197] S. Banerjee, C. Grosan, A. Abraham. "Intrusion detection on sensor networks using emotional ants". International Journal of Applied Science and Computations 2005; 12(3):152–173.

[198] E. Soroush,J. Habibi, MS. Abadeh. "Intrusion detection using a boosting ant colony based data miner". Proceedings of the 11th International CSI Computer Conference, Tehran, Iran, 2006; 563–566.

[199] T.V. Phuong, L.X. Hung, S.J. Cho, Y.K. Lee, S.Y. Lee. "An Anomaly Detection Algorithm for Detecting Attacks in Wireless Sensor Networks", Intelligence and Security Informatics. Lecture Notes in Computer Science, 2006, Vol. 3975/2006. Springer, 2006.

[200] Y. Ponomarchuk, D. W. Seo. "Intrusion detection based on traffic analysis in wireless sensor networks". 2010 19th Annual Wireless and Optical Communications Conference (WOCC), Shanghai, 2010; 1–7.

[201] B. David, T.R. de Sousa, Jr. "A Bayesian trust model for the MAC layer in IEEE 802.15.4 networks. I2TS 2010 - 9th International Information and Telecommunication Technologies Symposium, Rio de Janeiro, Brazil; 2010.

[202] M. Momani. "Bayesian fusion algorithm for inferring trust in wireless sensor networks". Journal of Network 2010; 5(7):815–822.

[203] X. Song,G. Chen, X. Li. "A weak hiddenMarkov model based intrusion detection method for wireless sensor networks". 2010 International Conference on Intelligent Computing and Integrated Systems (ICISS), Guilin, 2010; 887–889.

[204] W. Xiong, C. Wang. "Feature selection: A hybrid approach based on self-adaptive ant colony and support vector machine". International Conference on Computer Science and Software Engineering,Wuhan, Hubei, 2008; 751–754.

[205] S. Kaplantzis , A. Shilton, N. Mani, Y. A. Sekercioglu. "Detecting selective forwarding attacks in wireless sensor networks using support vector machines". 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007, Melbourne, Qld, 2007; 335–340.

[206] P. Kabiri, A. A. Ghorbani. "Research on intrusion detection and response: A survey". International Journal of Network Security 2005; 1(2):84–102.

[207] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, S. Zhou. "Specification-based anomaly detection: a new approach for detecting network intrusions". Proceedings of the 9th ACM Conference on Computer and Communications Security, ACM: Washington, DC, USA, 2002; 265–274.

[208] N. Stakhanova, S. Basu,J. Wong. "On the symbiosis of specification-based and anomaly-based detection". Computers Security 2010; 29(2010):253–268.

[209] P. Ning, K. Sun. "How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols". Information Assurance Workshop, 2003, IEEE Systems, Man and Cybernetics Society North Carolina State, 2003; 60–67.

[210] C. Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, K. Levitt. "A specification-based intrusion detection system for AODV". SASN '03 Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, New York, 2003; 125–134.

[211] J. Grönkvist, A. Hansson, M. Sköld. "Evaluation of a specification-based intrusion detection system for AODV". The Sixth Annual Mediterranean Ad Hoc Networking WorkShop, Corfu, Greece, 2007; 121–128.

[212] C. H. Tseng, T. Song, P. Balasubramanyam, C. Ko, K. N Levitt. "A specification-based intrusion detection model for OLSR". Recent Advance in Intrusion Detection RAID 2005; 2005:330–350.

[213] J. M. Orset, B. Alcalde, A. Cavalli. "An EFSM-based intrusion detection system for ad hoc networks". In Lecture Notes in Computer Science, Vol. 3707/2005. Springer-Verlag: Berlin Heidelberg, 2005; 400–413.

[214] L. Mostarda, A. Navarra. "Distributed intrusion detection systems for enhancing security in mobile wireless sensor networks". International Journal of Distributed Sensor Networks 2008; 4:83–109.

[215] A. H. Farooqi and F. A. Khan, "Intrusion Detection Systems for Wireless Sensor Networks: A Survey," in Communication and Networking, D. Ślęzak, T. Kim, A. C.-C. Chang, T. Vasilakos, M. Li, and K. Sakurai, Eds. Springer Berlin Heidelberg, 2009, pp. 234–241.

[216] I. Butun, S. D. Morgera, and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," IEEE Commun. Surv. Tutor., vol. 16, no. 1, pp. 266–282, 2014.

[217] F. Liu, X. Cheng, and D. Chen, "Insider Attacker Detection in Wireless Sensor Networks," in IEEE INFOCOM 2007. 26th IEEE International Conference on Computer Communications, 2007, pp. 1937–1945.

[218] G. Li, J. He, and Y. Fu, "Group-based intrusion detection system in wireless sensor networks," Comput. Commun., vol. 31, no. 18, pp. 4324–4332, Dec. 2008.

[219] A. Stetsko, L. Folkman, and V. Matyáš, "Neighbor-Based Intrusion Detection for Wireless Sensor Networks," in 2010 6th International Conference on Wireless and Mobile Communications (ICWMC), 2010, pp. 420–425.

[220] H. Sedjelmaci, S.-M. Senouci, and M. Feham, "Intrusion detection framework of cluster-based wireless sensor network," in 2012 IEEE Symposium on Computers and Communications (ISCC), 2012, pp. 000893–000897.

[221] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," IEEE Commun. Surv. Tutor., vol. 11, no. 4, pp. 42–56, Fourth 2009.

[222] M. K. G. Sharma Kalpana, "Wireless Sensor Networks: An Overview on its Security Threats," Int. J. Comput. Appl., 2010.

[223] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Comput., vol. 7, no. 1, pp. 74–81, Jan. 2008.

A

Thesis publications

A.1 International journals

- "6lo technology for smart cities development: Security case study"
- A. RGHIOUI, A. KHANNOUS, S. BOUCHKAREN, Pr. M. BOUHORMA
- International Journal of Computer Application (IJCA)
- Indexed: ProQuest
- ISSN: 0975 - 8887
- DOI: 10.5120/16089-5402
- Volume 92 - Number 15
- Publisher: Foundation of Computer Science, New York, USA
- Published (April 2014)

————————————————-

- "Security Key Management Model for Low Rate Wireless Personal Area Networks"

- A. RGHIOUI, S. BOUCHKAREN, A. KHANNOUS, Pr. M. BOUHORMA
- International Journal of Computer Science and Security (IJCSS)
- Indexed: Directory of Open Access Journals (DOAJ)
- ISSN: 1985 - 1553
- Volume 8 - Issue 5
- Publisher: CSC Journals, Kuala Lumpur, Malaysia
- Published (October 2014)

————————————————-

- "Denial-of-Service attacks on 6LoWPAN-RPL networks: issues and practical Solutions"
- A. RGHIOUI, A. KHANNOUS, Pr. M. BOUHORMA
- Journal of Advanced Computer Science & Technology
- Indexed: ProQuest
- ISSN: 2227 - 4332
- DOI: 10.14419/jacst.v3i2.3321
- Publisher: Science Publishing Corporation, Bremen, Germany
- Published (December 2014)

————————————————-

- "Symmetric cryptography keys management for 6LoWPAN networks"
- A. RGHIOUI, R. ABDMEZIEM, S. BOUCHKAREN, Pr. M. BOUHORMA
- Journal of Theoretical and Applied Information Technology
- Indexed: Scopus - ID: 19700182903
- ISSN: 1992 - 8645

- Volume 73 - Number 3
- Publisher: JATIT, Islamabad, Pakistan
- Published (March 2015)

————————————————-

- "Protecting e-healthcare data privacy for Internet of Things based Wireless Body Area Network"
- A. RGHIOUI, Dr. A. L'AARJE, Pr. F. ELOUAAI, Pr. M. BOUHORMA
- Research Journal of Applied Sciences, Engineering and Technology
- Indexed: Scopus - ID: 19700187706
- ISSN: 2040 - 7459
- Volume 9 - Issue 6
- Publisher: Maxwell Scientific Publications, United Kingdom
- Published (April 2015)

————————————————-

- "Monitoring behavior-based Intrusion Detection System for 6LoWPAN networks"
- A. RGHIOUI, A. KHANNOUS, Pr. M. BOUHORMA
- International Journal of Innovation and Applied Studies (IJIAS)
- Indexed: Directory of Open Access Journals (DOAJ)
- ISSN: 2028 - 9324
- Publisher: ISSR Journals, Rabat, Morocco
- Published (June 2015)

A.2 International conferences

- "Analytical study of security aspects in 6LoWPAN networks"
- A. RGHIOUI, Pr. M. BOUHORMA, Pr. A. BENSLIMANE
- Information and Communication Technology for the Muslim world (ICT4M 2013)
- 25th -27th March 2013 - Rabat
- IEEE conference
- published in IEEEXplore Degital Library
- ISBN: 978-1-4799-0134-0
- DOI: 10.1109/ICT4M.2013.6518912
- Oral communication

———————————————-

- "Securing Bootstrapping Phase in Distributed LR WPA IEEE 802.15.4-based Networks"
- A. RGHIOUI, S. BOUCHKAREN, A. KHANNOUS, Pr. M. BOUHORMA
- International Workshop on Wireless Technologies and Distributed Systems (WITS 2014)
- 9th - 10th April 2014 - Fez
- Published in conference proceedings
- Oral communication

———————————————-

- "Securing private wireless sensors in a shared environment in the internet of things context"
- A. RGHIOUI, S. BOUCHKAREN, A. KHANNOUS, Pr. M. BOUHORMA

- National Security Days (JNS 2014)
- 12th - 13th May 2014 - Tetuan
- IEEE conference
- published in IEEEXplore Degital Library
- ISBN: 978-1-4799-5586-2
- DOI: 10.1109/JNS4.2014.6850126
- Oral communication

————————————————-

- "Proposed Security Schema For 6LoWPAN Networks"
- A. RGHIOUI, Pr. M. BOUHORMA
- Colloque International de Cybercriminalité (CIC 2014)
- 24th - 25th June - Kenitra
- Published in conference proceedings
- Poster

————————————————-

- "The Internet of Things for Healthcare Monitoring Security Review and Proposed Solution"
- A. RGHIOUI, Dr. A. L'AARJE, Pr. F. ELOUAAI, Pr. M. BOUHORMA
- Conference on Information Systems and Technology - Internet of Things (CIST - IoT 2014)
- 20th - 22th October 2014 - Tetuan
- IEEE conference
- published in IEEEXplore Degital Library
- ISBN: 978-1-4799-5978-5

- DOI: 10.1109/CIST.2014.7016651
- Oral communication

————————————————-

- "Intrusion detection architecture for 6LoWPAN networks based on neighbor behavior surveillance"
- A. RGHIOUI, Y. ALLUHAIDAN, Pr. M. BOUHORMA
- International Conference on Cybercrime (CIC 2015)
- 4th - 5th June 2015 - Tetuan
- Published in Mediterranean Telecommunication Journal
- Oral communication

A.3 National conferences

- "Mesures Contre Les Menaces De Sécurité Ciblantes Le Routage Des Réseaux 6LoWPAN"
- La 2ème Rencontre des Jeunes Chercheurs (2RJC 2013)
- 25th - 26th May 2013 - Tetuan
- Published in conference proceedings
- Oral communication

————————————————-

- "Smart City Applications in the Internet of Things Context: Security Analysis"
- La 15ème Journée de la Recherche de l'Université Abdelmalek Essaadi (15 JR-UAE 2013)
- 20th - 21th December 2013 - Tetuan
- Poster

———————————————————-

- ”Contribution aux réseaux 6LoWPAN: Spécifications d’un système de détection d’intrusion”
- La 3ème Rencontre des Jeunes Chercheurs (3RJC 2014)
- 29th -31th May 2014 - Tetuan
- Published in conference proceedings
- Oral communication

———————————————————-

- ”Internet of Things for Healthcare Monitoring: Applications and Security Challenges”
- La 3ème Rencontre des Jeunes Chercheurs (3RJC 2014)
- 29th -31th May 2014 - Tetuan
- Published in conference proceedings
- Poster

———————————————————-

- ”Approche de sécurité pour les réseaux à faibles ressources dans le domaine de l’Internet des Objets”
- Séminaire 4 de La Campagne Nationale de Lutte Contre la Cybercriminalité (CNLCC 2014) Tétouan
- 14th June 2014 - Tetuan
- Oral communication

A.4 Collaborations

- Pr. A. BENSLIMANE
  Laboratoire d'Informatique d'Avignon
  Avignon, France
- Mr. R. ABDMEZIEM
  Laboratoire des Systèmes d'Informatiques
  Alger, Algeria
- Mr. Y. A. ALLUHAIDAN
  Saudi Business Machines
  Riyadh, Saudi Arabia
- Dr. A. L'AARJE
  Centre Hospitalier Universitaire
  Casablanca, Morocco
- Mr. S. BOUCHKAREN
  Laboratoire des Technologies de l'Information et de la Communication
  Tangier, Morocco
- Mr. A. KHANNOUS
  Laboratoire d'Informatique, Systèmes et Télécommunications
  Tangier, Morocco

B

AVISPA simulations

B.1 LoWPAN key evaluation

The HLPSL code is:

```
role role_R(R:agent,IdN:text,SND,RCV:channel(dy))
played_by R
def=
local
State:nat,Ts:text,S:text,Te:text,
Ker:symmetric_key,Krn:symmetric_key
init
State := 0
transition
1. State=0 /\ RCV({S'.Ts'.Te'}_Ker')
   =|> State':=1
4. State=1 /\ RCV({{IdN}_Krn'}_Ker)
   =|> State':=2
end role
```

```
role role_E(E:agent,S:text,SND,RCV:channel(dy))
played_by E
def=
local State:nat,Te:text,Ts:text,
Ker:symmetric_key,IdN:text,Krn:symmetric_key
init
State := 0
transition
1. State=0 /\ RCV(start) =|> State':=1
/\ Ker':=new() /\ Te':=new() /\ Ts':=new()
/\ SND({S.Ts'.Te'}_Ker') /\ SND(S.Ts'.Te')
3. State=1 /\ RCV({IdN'}_Krn') =|> State':=2
/\ SND({{IdN'}_Krn'}_Ker)
end role

role role_N(N:agent,IdN:text,SND,RCV:channel(dy))
played_by N
def=
local State:nat,Te:text,S:text,Ts:text,Krn:symmetric_key
init
State := 0
transition
2. State=0 /\ RCV(S'.Ts'.Te')
   =|> State':=1 /\ Krn':=new() /\ SND({IdN}_Krn')
end role
role session1(S:text,E:agent,R:agent,N:agent,IdN:text)
def=
local
SND3,RCV3,SND2,RCV2,SND1,RCV1:channel(dy)
composition
role_N(N,IdN,SND3,RCV3)
/\ role_E(E,S,SND2,RCV2)
/\ role_R(R,IdN,SND1,RCV1)
end role

role environment()
def=
```

```
const
r:agent,s:text,e:agent,n:agent,
const_1:text,auth_1:protocol_id
intruder_knowledge = {}
composition
session1(s,e,r,n,const_1)
end role

goal
authentication_on auth_1
end goal

environment()
```

B.2 Inter-LoWPAN key evaluation

The HLPSL code is:

```
role role_R(R:agent,IdM:text,Ker:symmetric_key,
Krn:symmetric_key,Krm:symmetric_key,SND,RCV:channel(dy))
played_by R
def=
local
State:nat,Kn:symmetric_key
init
State := 0
transition
3. State=0 /\ RCV({{IdM.Kn'}_Krn}_Ker)
   =|> State':=1 /\ SND({{Kn'}_Krm}_Ker)
end role

role role_E(E:agent,S:text,Ker:symmetric_key,
SND,RCV:channel(dy))
played_by E
def=
```

```
local
State:nat,IdM:text,Krn:symmetric_key,
Krm:symmetric_key,Kn:symmetric_key
init
State := 0
transition
2. State=0 /\ RCV({IdM'.Kn'}_Krn')
   =|> State':=1 /\ SND({{IdM'.Kn'}_Krn'}_Ker)
4. State=1 /\ RCV({{Kn}_Krm'}_Ker)
   =|> State':=2 /\ SND({Kn}_Krm')
end role

role role_N(N:agent,Krn:symmetric_key,
Kn:symmetric_key,SND,RCV:channel(dy))
played_by N
def=
local
State:nat,IdM:text,T:text
init
State := 0
transition
1. State=0 /\ RCV(IdM')
   =|> State':=1 /\ SND({IdM'.Kn}_Krn)
6. State=1 /\ RCV({T'}_Kn)
   =|> State':=2
end role

role role_M(M:agent,IdM:text,Krm:symmetric_key,
SND,RCV:channel(dy))
played_by M
def=
local
State:nat,Kn:symmetric_key,T:text
init
State := 0
transition
1. State=0 /\ RCV(start)
   =|> State':=1 /\ SND(IdM)
```

```
5. State=1 /\ RCV({Kn'}_Krm)
   =|> State':=2 /\ T':=new() /\ SND({T'}_Kn')
end role

role session1(Kn:symmetric_key,Krn:symmetric_key,
N:agent,R:agent,E:agent,S:text,Ker:symmetric_key,
M:agent,IdM:text,Krm:symmetric_key)
def=
local
SND4,RCV4,SND3,RCV3,SND2,RCV2,SND1,RCV1:channel(dy)
composition
role_M(M,IdM,Krm,SND4,RCV4)
/\ role_N(N,Krn,Kn,SND3,RCV3)
/\ role_E(E,S,Ker,SND2,RCV2)
/\ role_R(R,IdM,Ker,Krn,Krm,SND1,RCV1)
end role

role environment()
def=
const
const_1:text,m:agent,s:text,r:agent,
key4:symmetric_key,key2:symmetric_key,n:agent,e:agent,
key1:symmetric_key,key3:symmetric_key,auth_1:protocol_id
intruder_knowledge = {}
composition
session1(key2,key4,n,r,e,s,key1,m,const_1,key3)
end role

goal
authentication_on auth_1
end goal

environment()
```

Colophon

This thesis was typeset using LaTeX, originally developed by Leslie Lamport and based on Donald Knuth's TeX. The body text is set in 11 point Arno Pro, designed by Robert Slimbach in the style of book types from the Aldine Press in Venice, and issued by Adobe in 2007. A template, which can be used to format a PhD thesis with this look and feel, has been released under the permissive MIT (X11) license, and can be found online at github.com/suchow/ or from the author at suchow@post.harvard.edu.