Contrôle et surveillance par les Réseaux de Capteurs Corporels sans Fil (WBAN)

Tariq Benmansour

THÈSE EN COTUTELLE PRÉSENTÉE

POUR OBTENIR LE GRADE DE

DOCTEUR DE

L'UNIVERSITÉ DE BORDEAUX
ET DE L'UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE

ÉCOLE DOCTORALE MATHEMATIQUES ET INFORMATIQUE

SPÉCIALITÉ INFORMATIQUE

Par Tariq BENMANSOUR

Contrôle et surveillance par les Réseaux de Capteurs Corporels sans Fil (WBAN)

Sous la direction de Pr. Toufik AHMED (Bordeaux INP) et de Pr. Samira MOUSSAOUI (USTHB).

Soutenue le 14 décembre 2020.

Membres du jury :

M.	BADACHE Nadjib	Professeur, USTHB	Président
M.	AHMED Toufik	Professeur, Bordeaux INP	Directeur de Thèse
Mme.	MOUSSAOUI Samira	Professeur, USTHB	Directrice de Thèse
M.	FOUCHAL Hacene	Professeur, U. Reims Champagne-Ardenne	Rapporteur
M.	BITAM Salim	Professeur, U. Biskra	Rapporteur
M.	LAGRANGE Xavier	Professeur, IMT Atlantique	Examinateur
Mme.	DOUKHA Zouina	MCB, USTHB	Invitée

TITRE : CONTROLE ET SURVEILLANCE PAR LES RESEAUX DE CAPTEURS CORPORELS SANS FIL (WBAN)

Résumé :

Le déploiement de biocapteurs sur le corps humain, en vue de la collecte des données physiologiques constitue ce qui est appelé un réseau de capteurs corporel sans fil ou Wireless Body Area Network (WBAN). Ainsi, pour assurer les communications entre les diffèrent composants des WBANs, l'organisme IEEE a établi la norme IEEE 802.15.6, comme norme de communication optimisée pour les terminaux et capteurs exigeants de faible consommation énergétique et fonctionnants dans ou autour du corps humain (mais non limitée aux humains). Dans ce contexte, plusieurs études de simulation ont été menées dans la littérature pour analyser et évaluer les performances du protocole d'accès CSMA/CA de la norme IEEE 802.15.6. De plus, des efforts ont été faits en matière de modélisation de ce protocole afin de mieux analyser les caractéristiques de la norme dans un contexte plus général. Cependant, ces modèles sont partiellement applicables aux applications WBANs qui présentent des trafics réseaux hétérogènes. Cette thèse porte sur la modélisation de la norme IEEE 802.15.6 dans le but de fournir un moyen d'évaluation et d'analyse de cette norme dans divers conditions et situations. Nous avons essayé, à travers les principales contributions réalisées dans le cadre de cette thèse de combler les lacunes des travaux existants comme suit : la première contribution concerne une évaluation des performances de la norme IEEE 802.15.6 utilisant de nombreuses stratégies de gestion des files d'attentes, dans un cadre médical réaliste (surveillance à domicile d'un patient souffrant d'un problème cardiaque). La deuxième contribution propose un modèle de gestion de file d'attente LLQ (Low Latency Queuing) comme complément au protocole CSMA/CA afin de répondre efficacement aux exigences du standard en termes de la Qualité de Service (QoS) pour certains types d'applications. La troisième contribution porte sur la proposition d'un modèle analytique permettant l'étude des performances du protocole d'accès CSMA/CA de la norme IEEE 802.15.6, en termes de latence et du taux de délivrance des paquets, sous l'hypothèse que les WBANs sont composés de nœuds hétérogènes qui génèrent un trafic hétérogène en termes de priorité. La dernière contribution traite la problématique de sécurité dans les réseaux WBANs. Elle propose un protocole de sécurité appelé "Server-Based Secure Key Management for the IEEE 802.15.6 standard" (SBSKM) qui permet au standard de pallier à la vulnérabilité d'usurpation d'identité, par l'inclusion d'un serveur de confiance, responsable de la création, de l'initialisation et de la distribution des clés de chiffrement et de leur renouvellement, ainsi que de garantir l'identité des capteurs qui se joignent au réseau. Mots-clés: réseaux de capteurs corporels (WBANs), IEEE 802.15.6, processus de renouvèlement et de récompense, files d'attente avec priorité, attaques d'usurpation d'identité.

Mots clés : Les réseaux de capteurs corporels, La sécurité des WBANs, La couche MAC, la Norme IEEE 802.15.6.

TITLE: CONTROL AND MONITORING BY WIRELESS BODY AREA NETWORKS (WBANS)

Abstract:

The deployment of several biosensors on the human body for the collection of physiological data forms what is called a Wireless Body Area Network (WBAN). Thus, to ensure wireless communications between the different components of WBANs, the IEEE has established the IEEE 802.15.6 standard, which is an optimized communication standard for low-power devices that operate on, in, or around the human body (but not limited to humans). In this context, several simulation studies have been conducted in the literature to analyze and evaluate the performance of the IEEE 802.15.6 CSMA/CA access scheme. Also, efforts have been made to model this scheme to better analyze the characteristics of the standard in a more general context. However, these models are partially applicable to WBANs applications with heterogeneous network traffic. This thesis deals mainly with a challenge related to the modeling of the IEEE 802.15.6 standard to provide a tool for evaluation and analysis of this standard in various channel conditions and situations. We have tried, through the main contributions made in this thesis, to address the shortcomings noted in existing work as follows: the first contribution concerns an evaluation of the performance of the IEEE 802.15.6 standard using numerous queue management strategies, in a realistic medical setting (home monitoring of a patient with a heart problem). The second contribution proposes an LLQ (Low Latency Queuing) queue management model as a complement to the CSMA/CA protocol to efficiently meet the requirements of the standard in terms of Quality of Service (QoS) for certain types of applications. The third contribution deals with the proposal of an analytical model allowing the study of the CSMA/CA access scheme of the IEEE 802.15.6 standard, in terms of latency and packet delivery rate under the assumption that WBANs are composed of heterogeneous nodes and that each of them generates heterogeneous traffic in terms of priority. The last contribution proposes a security protocol called "Server-Based Secure Key Management for the IEEE 802.15.6 standard" (SBSKM) that allows the standard to address the vulnerability of impersonation attacks, by including a trusted server, responsible for the creation, initialization, and distribution of encryption keys and their renewal, as well as to guarantee the identity of sensors joining the network. Keywords: Body Area Networks (WBANs), IEEE 802.15.6 standard, renewal reward process, priority queues, and impersonation attacks.

Keywords: Wireless Body Area Networks, WBANs security, MAC layer, IEEE 802.16.6 standard.

RESUME DE THESE

Les récents progrès enregistrés dans le domaine des communications sans fil et dans l'industrie des composants électroniques ont permis le développement d'une large gamme de biocapteurs miniatures et performants. Ceci, représente un grand intérêt auprès de la communauté de recherche en raison de leurs vastes domaines d'application, notamment ceux de la santé, du sport, des loisirs, du bien-être, etc. Le déploiement de plusieurs biocapteurs sur ou dans le corps humain, en vue de collecter des données physiologiques forme ce qu'on appelle un réseau de capteurs corporel sans fil - Wireless Body Area Network. Ces biocapteurs portables (voir implantés), communiquent les données collectées à un nœud central appelé le BNC (Body Network Coordinator) via une technologie sans fil afin d'être réexpédiées en temps réel vers un hôpital, une clinique ou un centre de traitement. Les WBANs sont généralement utilisés pour la surveillance des personnes âgées, à mobilité réduite, à risques, ou ayant des maladies chroniques. Ils permettent aussi le suivi des patients en temps réel pour intervenir le plus rapidement possible dans les cas d'urgences.

Les WBANs peuvent être vus comme étant des Réseaux de Capteurs Sans Fil (RCSFs) caractérisés par de nouvelles contraintes à savoir : l'approche de déploiement (déterministe, aléatoire), la densité des nœuds, la périodicité et la corrélation de phénomènes physiologiques observés (ex : lorsqu'un patient est malade, tous les capteurs des phénomènes physiologiques -température, hypertension, battement du cœur se déclenchent et envoient en parallèle leurs données à la station de traitement, tandis que dans l'état normal les capteurs envoient leurs données périodiquement), la mobilité des nœuds causée principalement par les mouvements du corps humain, l'hétérogénéité des nœuds en terme de ressources (ex : les ressources d'énergie des nœuds implantés sous la peau sont bien inférieures à ceux attachées aux vêtements) et en terme de fonctionnalité (ex : les capteurs de température, de glycémie, d'hypertension, de vidéo, etc.).

Dans nos jours, de nombreuses normes sans fil, telles que: IEEE 802.11[2], IEEE 802.15.1[3] et IEEE 802.15.4 [4], sont utilisées pour assurer les communications entre les différents composants des WBANs. Cependant, ces normes ne peuvent pas répondre à l'intégralité des contraintes qui caractérisent les WBANs, du fait qu'elles sont conçues pour d'autres environnements réseaux ayant des caractéristiques physiques différentes (Ad-Hoc, WSNs et WPANs) à celles des WBANs. En 2007, l'organisme IEEE a créé le «Task Group 6» au sein du groupe de travail IEEE 802.15 avec pour mission de se concentrer sur des technologies sans fil pouvant opérer à proximité ou au sein du corps humain. Les résultats des travaux de ce groupe ont abouti à l'établissement de la norme IEEE

802.15.6, qui est une norme de communication optimisée pour les appareils à basse consommation d'énergie et qui fonctionnent sur, dans ou autour du corps humain (mais non limitée aux humains) pour servir une diversité d'applications, y compris médicales, divertissement et autres. La norme IEEE 802.15.6 offre un débit de données allant jusqu'à 10 Mbps. Afin de couvrir une large gamme d'applications des WBANs, la norme offre trois couches physiques différentes: une couche physique de la communication du corps humain (HBC: Human Body Communications), une couche physique à bande étroite (NB: NarrowBand) et une couche physique à bande ultralarge (UWB: Ultra-WideBand). En outre, la norme présente un superframe au niveau de la couche MAC avec une structure plus flexible qui prend en charge plusieurs modes d'accès au canal [7].

Plusieurs études de simulation ont été menées dans la littérature pour analyser et évaluer les performances du protocole d'accès CSMA/CA de la norme IEEE 802.15.6. De plus, des efforts ont été consentis en matière de modélisation de ce protocole afin de mieux analyser les caractéristiques de la norme dans un contexte plus général, sans se limiter à des scénarios prédéfinit et limités comme dans les études par simulation. Comme c'était le cas pour les modèles analytiques proposés pour les normes de communication sans fil antérieures, la modélisation de la procédure de Backoff du protocole CSMA/CA de la norme IEEE 802.15.16 se base principalement sur les chaînes de Markov discrètes ou sur les processus de renouvellement. La modélisation de la norme a fait l'objet de plusieurs études [8], [9], [10], [11], [12], [13], [14] et [15], tandis que, la plupart de ces modèles analytiques traitent le trafic hétérogène dans les WBANs d'une manière globale tout en supposant que chaque nœud du réseau ne peut générer et traiter qu'un seul type de trafic. Cette hypothèse n'est pas en adéquation avec la norme IEEE 802.15.6 qui permet de générer un trafic hétérogène en termes de priorités par le même nœud capteur (trafic médical, trafic de contrôle, rapports d'événements des nœuds de capteurs...). Par conséquent, ces modèles ne peuvent pas être utilisés pour l'étude de toutes les applications possibles des WBANs utilisant la norme IEEE 802.15.6 comme technologie de communication.

D'autre part, la récolte de données physiologiques des individus sous surveillance, leur transfert vers des serveurs distants pour le traitement, le stockage et le suivi ont créé de nouvelles inquiétudes au sein des utilisateurs de ce genre de technologies, en particulier pour ce qui se rapporte à la protection de leur vie privée. Bien que la sécurité soit une priorité dans ce cas, peu d'études ont été effectuées dans ce domaine pour les WBANs en raison de contraintes strictes liées aux ressources, notamment en termes de puissance, de mémoire, de débit de communication et de capacité de calcul.

L’objectif principal des travaux réalisés dans le cadre de cette thèse est de combler les lacunes des travaux existants en proposant de nouvelles solutions pour les problématiques de recherche identifiées. Cette thèse porte sur un défi lié principalement à la modélisation de la norme IEEE 802.15.6 dans le but de fournir un moyen d’évaluation et d’analyse de cette norme dans divers conditions et situations. Les principales contributions de cette thèse sont résumées comme suit :

Contribution 1 [16]**:**

Nous avons évalué les performances de la norme IEEE 802.15.6, dans un scénario médical réel (surveillance à domicile d'un patient souffrant d’un problème cardiaque). Ce scénario (description, contraintes et exigences) est défini selon la norme ISO/IEEE 11073. Cette dernière définit plusieurs cas d’utilisation afin d’évaluer les protocoles de communication sans fils dans des contextes réels. Dans un premier lieu, nous avons étudié les performances du protocole d’accès au canal CSMA/CA de la norme IEEE 802.15.6, en faisant varier la longueur de la phase Exclusive Access Phase (EAP), destinée au trafic urgent, et la priorité des paquets. Ensuite, une analyse comparative des performances des protocoles d’accès au canal proposés par IEEE 802.15.4 et IEEE 802.15.6 a été conduite.

Contribution 2 [17]**:**

Pour garantir une meilleure QoS des données transmises dans les WBANs, la norme IEEE 802.15.6 définit plusieurs types de priorité des paquets. Cette priorisation favorise les nœuds ayant des paquets urgents à accéder au canal avant les nœuds ayant des paquets ordinaires. Cependant, dans l’état de saturation, où chaque nœud détient au moins un paquet dans sa fil d’attente, cette norme ne définit ni la manière dont les paquets sont mis en file d'attente ni la façon dont ils sont sélectionnés au niveau de la couche MAC pour les transmettre. Dans cette contribution, nous avons évalué en premier lieu les performances de la norme IEEE 802.15.6 dans un contexte de surveillance d'un patient cardiaque, en utilisant de nombreuses stratégies de gestion des files d'attente. En deuxième lieu, nous avons proposé un modèle de gestion de file d’attente LLQ (Low Latency Queueing) comme un complément au protocole CSMA/CA afin de répondre aux objectifs de la norme IEEE 802.15.6 en termes de QoS.

Contribution 3 [18]:

Afin de produire un modèle analytique permettant l'étude du protocole d'accès CSMA/CA de la norme IEEE 802.15.6, en termes de latence et du taux de délivrance des paquets, nous avons proposé deux sous-modèles complémentaires. Tout d'abord, nous avons proposé un modèle analytique

décrivant le processus de Backoff du CSMA/CA de la norme IEEE 802.15.6. Ce modèle conclu sous l'hypothèse que les WBANs sont composés de nœuds hétérogènes et que chacun d'entre eux génère un trafic hétérogène en termes de priorité. Par la suite, nous avons proposé un modèle de gestion de file d'attente avec priorité pour répondre aux objectifs de la norme IEEE 802.15.6 en termes de QoS pour le trafic de priorité élevée. À partir du premier modèle le délai moyen écoulé pour exécuter la procédure de Backoff, qui s'étale de l'instant où le paquet quitte la file d'attente jusqu'à sa transmission complète ou sa suppression, est calculé. Ce délai servira comme temps de service pour notre modèle de gestion de file d'attente.

Contribution 4 [19]:

Comme dans toutes les applications informatiques utilisant des données liées à la santé de l'être humain, les WBANs peuvent transporter des informations sensibles, via des communications sans fil. Cette dernière peut exposer la vie des individus sous surveillance à plusieurs risques pouvant être fatals. La norme IEEE 802.15.6 offre une procédure d'association de sécurité afin d'identifier les nœuds capteurs et le BNC, l'un à l'autre. Cependant, de nombreuses vulnérabilités de sécurité ont été constatées dans cette procédure, notamment face aux attaques d'usurpation d'identité. Dans cette contribution, nous avons proposé un mécanisme de sécurité qui permet au standard de pallier à cette vulnérabilité, par l'inclusion d'un serveur de confiance, responsable de la création, de l'initialisation et de la distribution des clés de chiffrement et de leur renouvellement, ainsi que de garantir l'identité des capteurs qui se joignent au réseau. Cette solution sécurise les WBANs fonctionnant avec le standard IEEE 802.15.6 sans influencer ses performances dans un contexte médical. Le protocole proposé, appelé "Server-Based Secure Key Management for the IEEE 802.15.6 standard" (SBSKM), assure le chiffrement de toutes les communications entre les nœuds et le BNC dès le début de la procédure d'association de sécurité.

Mots-clés: Les réseaux de capteurs corporels (WBANs), La norme IEEE 802.15.6, la couche MAC, CSMA/CA, Le processus de renouvèlement et de récompense. Les files d'attente avec priorité, Les protocoles de routages dans les WBANs, Les attaques d'usurpation d'identité.

Thesis Publications

Journal Paper

- T. Benmansour, T. Ahmed, S. Moussaoui, and Z. Doukha, "Performance analyses of the IEEE 802.15.6 wireless body area network with heterogeneous traffic," J. Netw. Comput. Appl., p. 102651, Apr. 2020.

Conference Papers

- T. Benmansour, T. Ahmed, and S. Moussaoui, *"Performance Evaluation of IEEE 802.15.6 MAC in Monitoring of a Cardiac Patient," in 2016 IEEE 41st Conference on Local Computer Networks Workshops (LCN Workshops),* 2016, pp. 241–247.
- T. Benmansour, T. Ahmed, and S. Moussaoui, "Performance analyses and improvement of the IEEE 802.15.6 CSMA/CA using the low latency queuing," in *2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2017, pp. 1–6.
- T. Benmansour, S. Moussaoui, T. Ahmed, and O. Boutaghou, "Server-Based Secure Key Management for the IEEE 802.15.6 standard," *in 2020 IEEE Symposium on Computers and Communications (ISCC),* 2020, pp. 1–6.

Acknowledgments

All thanks and praise are due to Allah, who made me reach this state and gave me the ability to complete this work. Foremost, I would like to express my gratitude to my supervisors Prof. Toufik AHMED and Prof. Samira MOUSSAOUI for their continuous support of my study and research, for their patience, motivation, and their guidance. I sincerely thank them for their encouragement and the trust that they put in me.

I would also like to thank Dr. DOUKHA Zouina for her precious feedback during my research. I appreciate the time that she has devoted to reviewing my work meticulously and her precious advice and guidance. I am honored that she is a guest amidst the jury members.

I would like to thank and express my sincere appreciation to jury members headed by Pr. BADACHE Nadjib and consists of Pr. FOUCHAL Hacene, Pr. LAGRANGE Xavier, Pr. BITAM Salim for their time and effort devoted to read my thesis. I am very glad and honored to be examined by such high-level experts.

I would also like to thank my family: my parents Mohamed and Houria for supporting me throughout my life with their unconditional love, patience, and trust.

I also thank my wife for her encouragement. My angelic daughters: Meriem and Ayoub. My brothers and sisters: Read, Faycel, Chihab, Sara, Sihem, Aicha and my soulmate Sara.

TABLE OF CONTENTS

List of Figures

List of Tables

Motivation:

Recent advances in wireless communications and the electronic industry have allowed the development of a wide range of miniature and high-performance biosensors, which represents a great interest for the research community because of their wide field of application, particularly in: health, sport, entertainment, well-being, etc. The deployment of several biosensors on the human body to collect physiological measurements forms what is called a WBAN. These wearable biosensors (or implanted) communicate the collected data, via wireless technology, to a central node called the BNC. In turn, the latter forwards the received data to processing centers, hospitals, or clinics to be processed. WBANs are typically used for monitoring: elderly people, handicapped people, at-risk people, or chronically diseased people. They also allow real-time monitoring of patients to act as quickly as possible in emergency cases.

WBANs can be seen as Wireless Sensor Networks (WSNs) with new constraints such as deployment approach, network density, frequency, and the correlation of observed physiological phenomena (e.g. when a patient is ill, all physiological sensors - temperature, blood pressure, a heartbeat - are activated to send their critical data to the processing station at the same time. While in the normal state, sensors nodes send their data periodically), nodes mobility caused mainly by the human body movements, the heterogeneity of the nodes in terms of resources (e.g. the energy resources of subdermal implementable nodes are lower than wearable nodes), and in terms of function (e.g. sensors for temperature, blood pressure, hypertension, video, etc.).

The latest international standard for WBAN is the IEEE 802.15.6 which aims to standardize the MAC layer of WBANs operating in short-range wireless communications within the vicinity of, or inside, a human body. The standard supports a vast range of data rates for different applications and allows devices to operate on very low transmission power ensuring human safety by minimizing the Specific Absorption Rate (SAR).

Several simulation studies have been conducted in the literature to analyze and evaluate the performance of the IEEE 802.15.6 standard CSMA/CA access protocol. Besides, efforts have been made to model this protocol to better analyze the overall characteristics of the standard in a more general context, without being limited to predefined scenarios as in the simulation studies. As was the case with the analytical models proposed for previous wireless communication standards, the modeling of the Backoff process of the CSMA/CA protocol of IEEE 802.15.16 is based mainly on Discrete-

Time Markov chains (DTMC) or renewal reward processes. The modeling of the standard was the issue of several studies [7], [8], [9], [10], [11], [12], [13] and [14]. Whereas most of these analytical models deal with heterogeneous traffic in WBANs in a global manner while assuming that each node in the network can generate and process only a single type of traffic. This assumption is not coherent according to the IEEE 802.15.6 standard that allows generating heterogeneous traffic in terms of priorities by the same sensor node (medical traffic, management traffic, event reports, etc.). Therefore, these models cannot be used to study all possible applications of WBANs using the IEEE 802.15.6 standard as a communication technology.

On the other hand, gathering and sending physiological data from individuals under monitoring to distant servers for further processing, storage, or monitoring have created new concerns among users of such technologies, particularly in terms of privacy protection. Although security is a priority in these types of applications, few studies have been carried out in the security area for WBANs due to strict resource constraints, particularly in terms of power, memory, communication flow, and computing capacity.

Key contributions:

The main objective of the work carried out within this thesis is to fill the gaps in existing work by proposing new solutions for the identified research problems. This thesis deals mainly with a challenge related to the modeling of the IEEE 802.15.6 standard to provide a tool for evaluating and analyzing this standard under various conditions and situations. The main contributions related to this thesis are summarized as follows:

Contribution 1 [16]:

In this contribution, we evaluate the performance of the IEEE 802.15.6 standard in a real medical scenario (home monitoring of a cardiac patient). This scenario (description, constraints, and requirements) is defined by the ISO/IEEE 11073 standard, which defines several use cases to evaluate wireless communication protocols in real contexts. Firstly, we study the performance of the IEEE 802.15.6 CSMA/CA access scheme, by varying the length of the EAP phase, reserved exclusively for emergency traffic, and packets' user priority. In a second step, a comparative analysis of the performance of the channel access protocols proposed by the two standards: IEEE 802.15.4 and IEEE 802.15.6 was performed.

Contribution 2 [17]:

To ensure a high QoS of traffic within WBANs, the IEEE 802.15.6 standard defines several user priority types to packets to advantage nodes with emergency traffic to access the channel before nodes with ordinary traffic. However, in a saturation regime, where each node has at least one packet in its MAC queue, the standard does not define how packets are queued at the MAC layer or how they are scheduled. In this contribution, we evaluate in a first step the performance of the IEEE 802.15.6 standard under many queueing strategies. Then, we propose an adapted Low Latency Queueing (LLQ) model to match the CSMA/CA access scheme to meet the QoS objectives expected by the standard.

Contribution 3 [18]:

To provide a general analytical model to study the IEEE 802.15.6CSMA/CA access scheme in terms of latency and delivery rate, we propose in this contribution two complementary sub-models. In the first one, we propose an analytical model describing the Backoff process of the CSMA/CA as described by the IEEE 802.15.6 standard while assuming that WBANs are composed of heterogeneous nodes and that each of them generates heterogeneous traffic in terms of priority. In the second one, we propose a queueing model with priority to meet the IEEE 802.15.6 standard objectives in terms of ensuring QoS for high emergency traffic. From the first model, we calculate the average time of the Backoff process, which starts from the moment when the packet leaves the queue until its successful transmission or drop. This delay will be used as service time for the queueing model.

Contribution 4 [19]:

WBANs, as most health-related applications, can carry sensitive information via wireless communications that expose the monitored individual's safety to various risks, including death. The IEEE 802.15.6 standard provides a security association procedure to identify sensor nodes and the BNC to each other. However, many security vulnerabilities have been identified in this procedure, including impersonation attacks. In this contribution, we propose a security mechanism that allows the standard to deal with this vulnerability, by including a trusted server, responsible for the creation, initialization, and distribution of encryption keys and their renewal, The proposed protocol, called "Server-Based Secure Key Management for the IEEE 802.15.6 standard" (SBSKM), ensures the encryption of all communications between the nodes and the BNC from the beginning of the security association procedure. In addition to guaranteeing the identity of the sensors joining the network, the proposed solution enables the security of WBANs operating with the IEEE 802.15.6 standard without affecting its performance.

Organization of the Thesis:

This thesis is organized into eight chapters. Chapter 1 introduces the thesis by presenting the motivation, the key contributions, and the organization of the thesis. Chapter 2 provides an overview of WBANs including their architectures, their applications, and the most important challenges and issues of this type of network mainly the security and QoS. Chapter 3 presents an overview of the IEEE 802.15.6 standard, its description, the related CSMA/CA access channel protocol, and the security paradigm provided by the standard. It also presents a comprehensive survey of existing and relevant IEEE 802.15.6 performance evaluation models. Chapter 4 presents a performance evaluation of the IEEE 802.15.6 in the monitoring of a cardiac patient. Chapter 5 provides a queueing model evaluation with the IEEE 802.15.6. Chapter 6 presents a renewal theory-based analytical model for the contention access of IEEE 802.15.6 CSMA/CA. Chapter 7 presents our solution towards proposing a Server-Based Secure Key Management for the IEEE 802.15.6 standard. Chapter 8 concludes this thesis and presents some future work and research directions.

2 WIRELESS BODY AREA NETWORKS (WBANS)

A typical WBAN consists of several heterogeneous biosensors that are placed in different parts of the body and can be wearable or implanted. Each of them has specific requirements and is used for several missions. These devices are used to measure changes in a patient's vital signs and to detect emotions or human moods. The WBAN also includes a coordinator which is generally less energy-constrained and has more processing capacities. It is responsible for managing the network and collecting all data from the sensor nodes. The collected data should then be relayed from the patient to medical centers, quickly and reliably, to provide real-time medical diagnostic and allow him to make the right decisions. Sensor nodes continuously monitor large amounts of data, which must be processed efficiently to extract relevant information. Data processing must be structured hierarchically to maintain system efficiency and ensure data availability when needed.

WBANs can be used for many applications such as ubiquitous health, sports, and entertainment. WBANs have enormous potential to revolutionize the future of health monitoring by offering a diagnosis of many life-threatening diseases and providing real-time patient monitoring.

2.1 Differences between WBANs and WSNs:

The challenges facing WBANs are mainly similar to those of wireless sensor networks (WSNs). However, there are many differences between the two networks due to the complexity of the internal environment of the human body and the characteristics of the external environment surrounding the human body, which requires special attention. Some of these differences and properties are illustrated in the following Table and summarized in the following.

Networks	WBANs	WSNs
Deployment	Deterministic	Deterministic or random way
Network density	Low	High
Scale	Limited to the human body centimeters/meters)	Large scale area (kilometers)
Traffic	Most often periodic traffic	Most often irregular traffic
Node tasks	Homogeneous nodes performing a dedicated task (vibration sensors, sensors…etc.)	Nodes are heterogeneous and handle multiple tasks
Energy consumption	low	high
Latency	low	high
Node mobility	Mobile	Stationary

Table 1: Comparison between WBANs and WSNs

- **Deployment and density:** Heterogeneous wireless biosensors in WBANs are placed strategically on the human body with a deterministic manner, implanted or simply attached to clothing. These sensors will monitor specific human body vital signs such as body temperature, blood saturation, and oxygen level or information related to user's surrounding environment such as the ambient temperature, the daily exposure to airborne pollutants, and the oxygen level. WBANs do not use redundant nodes to deal with nodes failures. As a result, the number of nodes in WBANs is restricted. In contrast, in WSNs, nodes are homogenous and deployed randomly to perform similar sensing functions. They are often deployed in locations that are not easily accessible, which requires deploying more nodes to establish a fully connected and adaptable network to deal with nodes failure problems.

- **Transmission range:** The transmission power should be limited due to concerns on human body health while using WBANs and, consequently, the communication range must be limited, contrary to WSNs that use many transmission powers to deliver data.

- **Traffic rate:** Most of WSNs are used to monitor events that occur at irregular intervals. However, WBANs are used to measure physiological activities that can occur more periodically and can result in relatively stable data traffic.

- **Battery lifetime:** In the case of WBANs, replacing batteries for sensors is easier than WSNs in which sensor nodes may be physically inaccessible after deployment. Therefore, it is not necessary to increase the battery lifetime in WBANs' nodes, especially those placed on the body. However, for the implanted nodes, which should be small sized to be comfortably implanted without constraining users' mobility, the replacement and charging of those sensor nodes are generally difficult since it can lead to some human body discomfort. In this case, we must deploy sensors nodes with a high energy capacity.

- **Latency:** Latency in WBANs is lower compared to latency in WSNs, due to the size of the network and the reduced number of hops to reach the Sink. WSNs allow monitoring of large-scale areas while with WBANs only an area limited to a few meters is monitored.

- **Mobility:** Unlike WSNs' nodes which are usually stationary, WBANs' sensor nodes are deployed on the human body, which is in continuous mobility.

2.2 WBANs architecture:

The topology of any network corresponds to its architecture, defining how the devices are interconnected and giving the spatial representation of the network. For WBANs, several types of topologies are used, but the most common is the star topology.

In the star topology, all nodes can only exchange data with the WBAN coordinator, either directly or via relay nodes (Figure 1).This topology is very efficient in terms of network management and troubleshooting: a failure of one sensor node does not affect the overall performance of the network. However, the Sink that connects all the other nodes is a single point of failure: a failure at this level makes the whole network useless.

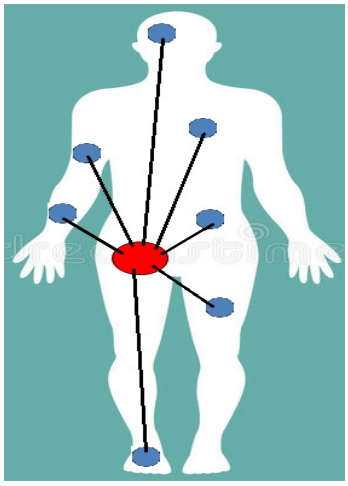

Figure 1: Star topology

In general, WBANs support three types of communication, namely, intra-WBAN communication, inter-WBAN communication, and beyond-WBAN communication. These different levels of communication are illustrated in Figure 2.

- **The Intra-WBAN communications:** Generally, a WBAN is organized into a star topology, where sensors nodes send their collected data to the BNC. Intra-WBAN communications refer to the communication between the different sensor nodes implanted or attached to the human body constituting the WBAN and the BNC. The latter is responsible for processing the collected data and managing the sensing nodes.
- **The Beyond-WBAN communications:** These types of communications are used to ensure reliable transmission of the collected data from the WBAN's coordinator node to a distant data center. The collected data is relayed through many intermediate devices, such as a Personal Digital Assistant (PDA), an Access Point (AP), or a mobile phone using several different communication technologies (WSNs, Wi-Fi, GPRS, UMTS, 4G, etc.).

- **The Inter-WBAN communications:** Due to the mobility of users equipped by WBANs and the frequent communication outages in environments and rural areas with insufficient coverage or unavailability of network infrastructure, it is not easy to relay the collected data reliably. In such a situation, WBANs involves inter-WBAN communication and exploits cooperative and multi-hop communication between BNCs to ensure reliable end-to-end data transmission by using short-range wireless technologies as ZigBee and Wi-Fi.

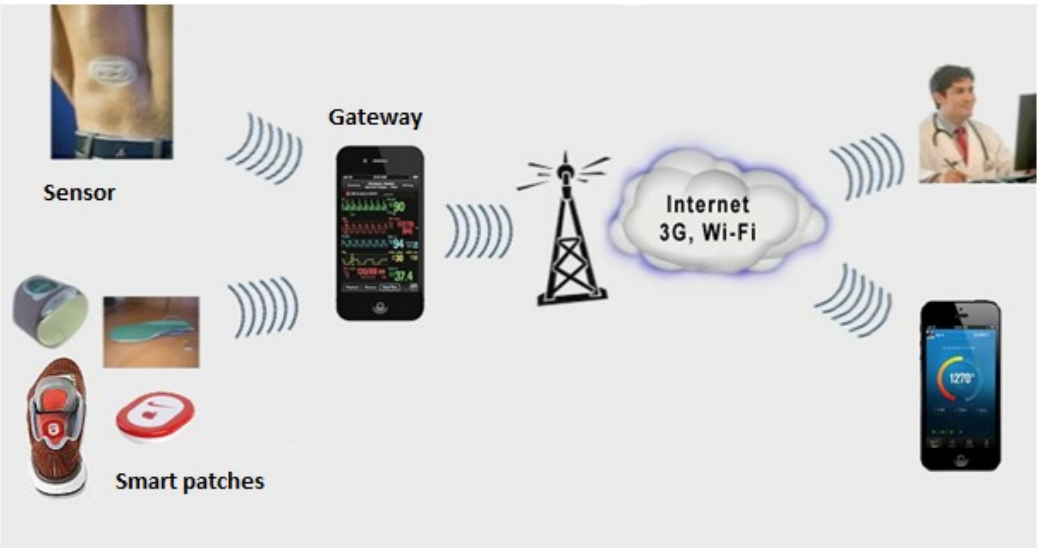

Figure 2: WBAN architecture

2.3 WBANs applications:

Due to technological advances in electronics and telecommunications fields that allowed the miniaturization of low-cost sensors, as well as the broadening of the range of available sensors (movement, temperature, etc.) and given their impact in improving the user's quality of life, WBANs applications are extended to several aspects and areas that are related to the human body and its surrounding environment. These applications can be classified mainly according to their use: medical or non-medical applications. Medical applications include health care systems designed mainly for the elderly and sick people. Typical examples of such applications are early detection, prevention, monitoring of diseases, administration of drugs, assistance to the elderly people at home, rehabilitation after surgery, and assistive living applications that improve the quality of life of people with handicaps. Non-medical applications include lifestyle, sport, and entertainment. Among these applications: motion and gesture detection for interactive games and fitness monitoring applications, cognitive and emotional recognition for driving assistance or social interaction, and useful information

in sport-related fields. For example, the sensory data of athletes' body movement can be examined to conserve energy and make the player perform at the maximum altitude over a long era of time.

2.4 WBANs communication technologies:

To date, many wireless standards such as IEEE 802.11 [2], IEEE 802.15.1[3], and IEEE 802.15.4 [4] are used for ensuring WBANs' communications. However, these standards are designed for environments having different characteristics (Ad-Hoc, WSN, and WPAN) compared to WBANs. Therefore, they cannot meet all WBANs' constraints. The power consumption of the IEEE 802.11 and IEEE 802.15.1, which can reach up to 800 mW and 100 mW respectively, is too high to respond to WBANs' low power nodes [20]. The IEEE 802.15.4 standard is the most used in WBANs. However, this standard cannot support high data rate applications either ensure data transmission of more than 250 Kbps [20][21]. Therefore, the IEEE Task Group 6 has been formed to standardize the MAC layer of WBANs operating in short-range wireless communications within the vicinity of, or inside, a human body [5]. That group provided the IEEE 802.15.6 standard, which supports QoS and allows devices to operate on very low transmission power, ensuring human safety by minimizing the Specific Absorption Rate (SAR) into the body and increasing the battery lifetime [5]. The IEEE 802.15.6 standard offers up to 10 Mbps data rate and it includes three different Physical Layers: Human Body Communications (HBC), Narrowband (NB) PHY, and Ultra-wideband (UWB) PHY to cover the broad range of monitoring applications. Besides, the standard presents a more flexible frame structure at the MAC layer that supports multiple channel access modes [6]. According to several studies such as [22], [23] and [24], the IEEE 802.15.6 standard is the more suitable for WBAN communications than other standards, especially for latency and reliability sensitive applications.

2.5 Challenges and issues of WBANs:

As we mentioned earlier, WBANs inherit the challenges and issues of WSNs. Also, they have more specific constraints due to their placement in and around the human body. These constraints require us to take the health of the body under observation as a priority when designing WBAN frameworks. In the following, the main WBANs challenges are described concisely, except for QoS and Security, which will be detailed since they have a directly related to our contributions presented in this thesis.

- **Network topology:**

The network topology describes how the different nodes communicate with each other. There are two main types of topology depending on the number of hops that packets must make from the source to the destination: single-hop topology and multi-hop topology. In single-hop topology, each node communicates directly with the destination node, while in multi-hop topology, data transmitted from the source nodes will pass through one or more intermediate nodes before reaching the destination node. Studies conducted in this field show that multi-hop topology is more reliable in terms of the number of packets delivered to the destination compared to single-hop topology[25]. In addition, multi-hop communications are much more resistant to frequent changes in network topology due to human body movements and short-range node transmissions.

- **Energy efficiency:**

WBANs are composed of miniature wireless sensor nodes implanted inside the human body, which makes it almost impossible to change their batteries. In a wireless network, wireless communications consume more energy than capture and processing operations.

- **Heterogeneous environment:**

The objective of the WBANs is to capture and monitor the different vital signs of the human body. Depending on the nature of the parameters to be observed, several types of nodes are used. Nodes can be distinguished in terms of computing resources, storage capacity, or energy consumption[26]. The heterogeneous nature of nodes imposes other challenges.

- **Biological effects:**

One of the most distinguished characteristics of WBANs is that the nodes are implanted inside or around the human body. This requires us to consider the unwanted effects of these networks on human health. The study conducted in[27] shows that transmitting and receiving data are the two distinct tasks that cause more heat in the vicinity of a node. Human tissues absorb the energy of radiation and convert it into heat, which causes an increase in temperature.

Radiation absorption is acceptable to the human body as long as it does not exceed a well-defined threshold. The most used parameter by international standards related to the electromagnetic safety of the human body is the *Specific Absorption Rate* (SAR). The IEEE standard recommends an average value of 1.6 W/kg per gram of tissue as the acceptable SAR value. This value is also adopted by the FCC (*Federal Communications Commission*)[27]. The effects of WBANs on the human body can be

reduced, by modifying on the design of nodes and their antennas on one hand, and adapting the design of routing protocols on the other hand to meet a safe SAR.

2.6 QoS and queueing in WBANs

In many WBANs applications, the QoS should be seriously taken, as they treat critical vital signs of the human body. The traffic can be classified into several categories (critical data, ordinary data, etc.) depending on the context of the application and the required QoS. One of the most important QoS metrics in WBANs is the latency, which is a critical parameter. Indeed, in some WBANs' applications, the packet has to be delivered from the source node to the destination node within a bounded time; otherwise, it becomes unnecessary and obsolete.

Due to transmission's limits caused by the high use of the medium, generated packets have to wait at sensor nodes MAC layer buffers until their transmission. This leads to the necessity of the use of efficient scheduling and queueing strategy. On the other hand, improving the QoS in WBANs, in particular by ensuring reliable and instantaneous delivery of emergency traffic requires the use of efficient service differentiation techniques. Several works have been presented in the literature to address this area of research, which includes various studies involving queueing strategies for service differentiation in WBANs. According to the level at which the traffic is buffered, we classify the related work into two major sub-classes namely: the queueing in intra-WBAN and the queueing beyond the WBAN.

a. *Queueing based models in intra-WBANs*:

The first class includes all literature studies that treat how packets are buffered at WBANs' sensor nodes before their transmission to the coordinator. In [35], the authors proposed a class-based QoS framework to provide low delay and maximum throughput for critical nodes in medical applications. The proposed framework performs service differentiation by categorizing packets by a classifier into three services classes (i.e. guaranteed service, real-time service, and best-effort service). Packets are en-queued in an adequate position of priority queue according to their assigned classes. In [36], the authors proposed a traffic differentiation and a scheduling scheme based on data prioritization. Through queues scheduling and path choice issues, emergency packets are delivered timely to the coordinator to provide a guarantee QoS for WBANs. After the classification phase, packets are en-queued in three queues (M/M/1) according to their priority class. Packets are scheduled from a tagged queue only if there is no data in the higher priority queues. In [37], the authors developed an analytical

framework to support low power body area networks. They defined three kinds of traffic coming to sensor nodes: critical traffic, streaming traffic, and non-critical traffic. To support WBANs' QoS, they considered three queues based on a G/M/1 model. In [13], the authors proposed a sleep mechanism for the IEEE 802.15.6 based WBANs, deployed in a hospital environment. To analyze lifetimes and delay requirements, they developed an analytical model for the IEEE 802.15.6 CSMA/CA Backoff process by using PGFs and Markovian techniques and they used an M/G/1 queue with repeated inhomogeneous vacations. In [8], [38], and [39], the authors provided several performance evaluations of the IEEE 802.15.6 standard under various channel conditions and traffic regimes. Authors proposed formal models for the CSMA/CA access scheme, based on the 3-dimensional DTMC, assuming that each node generates only one type of traffic, buffered in local MAC queue with infinite capacity. In [40], the authors proposed to use queues' lengths to provide a novel contention probability dynamism for the aim of improving the IEEE 802.15.6 slotted-ALOHA scheme. They assumed that each node treats only one type of traffic, buffered in its local queue. The authors in [41] provided a prioritized queueing mechanism for the IEEE 802.15.6 standard by defining three priority queues at the MAC layer. The goal of this prioritization is to guarantee minimum delay and more reliability. The authors showed by simulations that the latency of the emergency packets is improved. To minimize QoS degradations in multiple adjacent BANs scenarios, the authors of [42] supposed that each node buffers the traffic in local queues and exploited previous work on Q-CSMA/CA [43] to propose a queue-size and channel quality based adaptation of the Energy Detection Threshold (EDT) at the receiver nodes. In [17], the authors studied the impact of queueing strategies on the IEEE 802.15.6 based WBANs. Simulation results showed that Priority Queueing (PQ) and LLQ improve clearly the latency and packets delivery rate of those networks.

***b. Queueing based models beyond the WBANs*:**

The second class focuses on the queueing beyond the WBANs, where the traffic is buffered at the BNC or gateways before its transmission to external centers for further processing. In [44] and [45], the authors designed a priority aware architecture for health monitoring networks. Medical packets are divided into several priority classes according to their delay sensitivity and buffered at intermediate gateways until their transmission beyond the WBAN to external servers. The authors have used an M/D/K queueing model with priorities, with a Poisson arrival, a deterministic service time, and K servers (i.e., K channels). The proposed differentiation permits a priority transmission of critical packets over ordinary ones. In [46], the authors defined a bridging between the IEEE 802.15.6 based

WBANs and the IEEE 802.11e Enhanced Distributed Channel Access (EDCA) based WLAN. The proposed bridge operates as a BNC in collecting medical data from WBAN nodes and as an ordinary station in the Wireless Local Area Network (WLAN). At bridges, the eight different user priorities defined by the IEEE 802.15.6 are mapped to 4 different Access Categories (AC). Packets are differentiated according to the Arbitrary Inter-Frame Space (AIFS) and the Contention Window (CW) to be affected to the adequate AC. Packets of each AC are buffered at a dedicated MAC queue.

2.7 Security in WBANs:

As in WSNs applications, security and confidentiality are basic requirements of WBANs. However, It is impossible to apply traditional security and confidentiality techniques to this type of network, due to low energy, resource limitations, and other constraints [28]. The deployment of WBANs and the integration of practical security mechanisms require a whole knowledge of WBAN security requirements [29][30], which are summarized in the following table.

Requirements	Definition	Defense mechanisms
Data integrity	Data is transmitted in an unsecured WBAN, can be modified by an opponent before reaching the network coordinator	- Encryption - Key management - Preventing falsification
Confidentiality of data	Critical information can be intercepted, which can cause a considerable amount of damage to a patient when the data is published for illegal purposes	- Encryption - Key management - Secure routing - Preventing falsification - Trust management
Data freshness	An opponent has the ability to capture data in the transmissions and then replay it to create confusion for the WBAN coordinator. The freshness of the data ensures that the data is not reused and that their images are in order	- Prevent wormholes - Prevent DoS - Secure routing - Trust management
Availability	The availability of information from the patient to the doctor must always be ensured. An attack on availability in WBANs could result in the loss of vital information such as ECG, for example, leading to the possible death of a patient	- Prevent wormholes - Prevent DoS - Secure routing - Routing robustness
Data authentication	The coordinator must check that the data is sent by a trusted node and not by a fake one.	- Prevent wormholes - Prevent DoS - Secure routing - Prevent Sybil attacks

Secure location system	WBANs require a precise estimate of the patient's location. Failure may allow an attacker to report false locations or replay position reports	- Securing the location - Secure routing - Prevent wormholes - Trust management
Secure management	Secure management at the coordinator level is essential to distribute encryption keys to sensors. In case of an association, the BNC must be able to safely add and remove sensors	- Key management - Trust management - Secure routing

Table 2: Security requirements and mechanisms for WBANs [29][30]

2.7.1 Security Attacks in the WBANs:

WBANs are vulnerable to various types of security attacks. Depending on the security requirements mentioned above, these attacks can be classified into three different classes [31]; a) Service Integrity Attacks, b) Authentication Attacks, c) Network Availability Attacks. On the other hand, many classifications of WBAN security attacks refer to the OSI layer [32] as described in Table 3.

Layer	Attacks
Physical	**Jamming:** This is a type of attack that interferes with the radio frequencies that nodes use for communication.
	Tampering: Given physical access to a node, the attacker can extract cryptographic keys from the captured node, alter its circuit, modify the program codes, or even replace it with malicious code.
Data Link	**Collision:** occurs when two nodes attempt to transmit simultaneously on the same frequency.
	Resource exhaustion: Repeated collisions can also be used by an attacker to cause resource depletion.
Network	**Selective Forwarding:** In a multi-hop network for message communication, all nodes must transmit messages accurately. An attacker can compromise a node in such a way that it selectively sends some messages and deletes others.
	Sinkhole: The attacker makes a compromised node more attractive to its neighbors by falsifying routing information. The result is that neighboring nodes choose the compromised node as the next jump node to route their data. This type of attack makes selective transfer very simple, as all traffic from a large area of the network would flow through the compromised node.
	Hello Flood: This attack exploits the Hello packets that are required in many protocols to announce nodes to their neighbors. A laptop-class opponent can send this type of packet to all sensors in the network so that they believe that the

	compromised node belongs to their neighbors, this causes a large number of nodes sending packets to this imaginary neighbor.
Transport	**Flooding:** An attacker can repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes.
	De-synchronization: De-synchronization refers to the disruption of an existing connection. For example, an attacker may repeatedly user messages to an end host, forcing the host to request the retransmission of the missed frames. If the delay is correct, an attacker can degrade or even prevent the ability of end hosts to successfully exchange data, causing them to waste energy trying to recover from errors caused.
Application	**Submersion attack:** An attacker may attempt to submerge network nodes with sensor stimuli, causing the network to transfer large volumes of traffic to a base station. This attack consumes network bandwidth and node energy.
	Path-based DOS attack: This consists of injecting parasitic or replayed packets into the network at the sheet nodes. This attack can deprive the network of legitimate traffic, as it consumes resources on the way to the base station, preventing other nodes from sending data to the base station.
	Flooding (reprogramming): a network programming system allows remote reprogramming of nodes in deployed networks. If the reprogramming process is not secure, an intruder can hijack this process and take control of large parts of a network.

Table 3: Classification of attacks on WBANs [32]

2.7.2 The impersonation attack:

An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or a communications protocol. In WBANs, an authentication protocol must make negligible the probability that, for a given node A, an attacker C distinct from node A, carrying out the protocol and playing the role of A, can cause another node B to complete and accept A's identity. Many techniques and security solutions have been designed to prevent impersonation attacks in WBANs. Among them, key management techniques, which are considered as one of the efficient solutions. Key management is the set of methods and techniques which support the establishment, maintenance, and revocation of cryptographic keys between the interacting parties. The literature proposes several solutions based on a key management protocol to WBANs' impersonation vulnerabilities. These solutions are diverse and varied in terms of key generation, exchange, and

renewal, but also in terms of their adaptability to the target network. In [33], the authors proposed BARI+, which is a Biometric Based Distributed Key Management protocol for WBANs, it uses an individual's biometric data to generate the encryptions keys. Indeed, according to this protocol, biometric data have the property of being random, which, in the context of symmetric key generation and their refreshing, is a robust method. This protocol assumes that in the initial state, the sensor nodes are initialized with a secret key. After that, the protocol creates a pair of keys based on the biometric data that will be used for communications and will have a renewal cycle based on the frequency of use, to prevent cryptanalysis attacks. In [34], the authors proposed a key management protocol based on the assignment of a secret key based on a unique identifier to each sensor, it also envisages a Backend server managing several WBANs, as well as a security server guaranteeing the identity of each sensor against impersonation attacks. In this protocol, the sensor sends a key request to the security server, the latter responds to the Backend server, which is responsible for transmitting the key to the sensor. The security server represents the security focal point, as it is responsible for generating all the keys used by the protocol, which, delegates the key generation to a third party rather than at the expense of network resources.

2.8 Conclusion

In this chapter, we presented an overview of WBANs, their architecture and applications. We cited the wireless technologies used for communications in such networks such as IEEE 802.15.1, IEEE 802.15.4, and IEEE 802.15.6. After that, we presented the main challenges and issues related to WBANs because they have more specific constraints due to their placement in and around the human body, and we focused our analysis on QoS and security, for which a detailed study is provided.

3 IEEE 802.15.6 WBAN STANDARD

The IEEE 802.15.6 standard was developed by the IEEE association to accommodate the growing demand for short-range, wireless communication in the vicinity of, or inside a human body (but not limited to humans) and to accelerate diversified applications of WBAN worldwide. The standard organizes networks into sets of WBANs each of them is expected to have only one Body Network Coordinator (BNC) and multiple nodes. The standard offers one hop and two-hop topologies. In the one-hop topology, data is exchanged between nodes and the BNC directly, while in the two-hop topology, the BNC and nodes may use relay nodes to exchange data [5].

A BNC can operate in a beacon mode with superframe, non-beacon mode with superframe, or non-beacon mode without superframe. The first mode offers synchronization between the BNC and all WBAN nodes and a broad range of access modes. As shown in Figure 3, the frame structure in beacon mode with superframe is divided into seven (7) access phases; two Exclusive Access Phases (EAP), two Random Access Phases (RAP), two Managed Access Phases (MAP), and one Contention Access Phase (CAP). The BNC transmits a beacon B frame at the start of the superframe specifying the start and the end times of these access phases and another optional beacon B2 before the start of the CAP to provide group acknowledgment. By receiving the beacon frame, WBAN's nodes and the BNC will establish reference time ensuring synchronization between them. In the EAP, RAP, and CAP access phases, sensor nodes use a priority-aware CSMA/CA or S-ALOHA access scheme to gain contended allocation. EAP is only used for high priority traffic (emergency packets and/ or medical event report), while the RAP is used for all traffic whatever the priority. To allow continual invocation of CSMA/CA or S-ALOHA and improve channel utilization, a node starting the Backoff process for an emergency packet may consider the combined EAP1 and RAP1 as a single EAP1, and the combined EAP2 and RAP2 as a single EAP2. During the MAP, the BNC may arrange scheduled uplink/downlink/bilink allocation intervals, may provide unscheduled bilink allocation intervals, and may improvise Type-I immediate polled allocation intervals and posted allocation intervals [5].

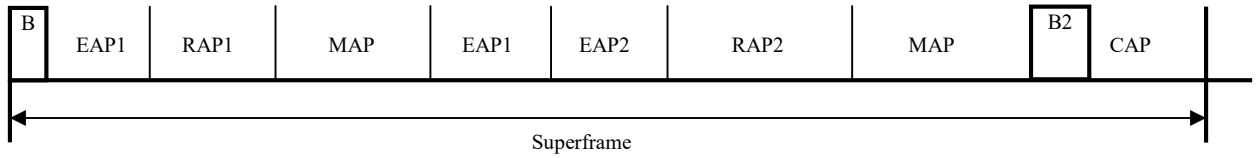

Figure 3: Superframe structure in beacon mode with superframe

3.1 IEEE 802.15.6 CSMA/CA access scheme:

In the IEEE 802.15.6 CSMA/CA access scheme, if a node has a priority-class-k packet to send, it sets its Backoff Counter (BC) to a random integer uniformly distributed over the interval [1, $W_{k,s}$], where $W_{k,s}$ represents the Contention Window at the s^{th} transmission attempt (Backoff stage). To send a priority-class-k packet, the node starts the Backoff process by setting the contention window $W_{k,s}$ to $CW_{k,min}$. The node decrements its BC by one for each idle CSMA/CA slot. Once the BC reaches zero, the packet is transmitted over the medium. As described in the following equation, if the packet transmission fails, the node doubles its $W_{k,s}$ for an even number of failures and keeps it unchanged for an odd number. If the doubling of the $W_{k,i}$ exceeds $CW_{k,max}$, the node sets its $W_{k,s}$ to $CW_{k,max}$.

$$W_{k,s} = \begin{cases} CW_{k,min} & if\ \ s = 0 \\ Min\left(2W_{k,s-1}, CW_{k,max}\right) & if\ 2 \le s \le m_k\ and\ s\ even \\ W_{k,s-1} & if\ 1 \le s \le m_k\ and\ s\ odd \\ CW_{k,max} & if\ \ m_k < s \le R. \end{cases} \quad (1)$$

Where, R stands for the maximum authorized transmission try and m_k represents the Backoff stage after which the contention window reaches its maximal value.

The values of $CW_{k,min}$ and $CW_{k,max}$ are defined by the standard according to data classes as presented in Table 4. The traffic is differentiated according to its type, ranging from Background traffic to the most critical emergency traffic. By assigning the highest user priority for emergency traffic and medical implant event reports, and low user priorities for the normal traffic, the proposed traffic differentiation leads to allow a timely transmission for high emergency traffic.

The IEEE 802.15.6 standard allows sensor nodes to lock and unlock their BC to avoid collisions and ensure the non-overlapping between superframe phases [5]. Nodes lock their BC in the following cases:

- The channel is busy because of a packet transmission of another node.
- The current time is outside any EAP,RAP or CAP phases.
- The current time is at the start of a CSMA slot within an EAP, RAP, or CAP, but the time between the end of the slot and the end of the EAP, RAP, or CAP is not long enough for completing the packet transmission.

Priority	UP (k)	Traffic designation	$CW_{k,min}$	$CW_{k,max}$
Lowest	0	Background	16	64
	1	Best effort	16	32
	2	Excellent effort	8	32
	3	Video	8	16
	4	Voice	4	16
	5	Medical data or network control	4	8
	6	High-priority data or network control	2	8
Highest	7	Emergency or medical implant event report	1	4

Table 4: Contention Window bounds and UP mapping for CSMA/CA

The node keeps locking its BC until both of the following conditions are met:

- The channel has been idle for $SIFS$ (Short InterFrame Spacing) within aEAP,RAP, or CAP.
- The time duration between the current time plus a CSMA/CA slot and the end of the EAP, RAP, or CAP is long enough for completing a packet transmission.

Each node decrements its BC by one for each idle slot. As shown in Figure 4, the node treats a CSMA/CA slot to be idle if the channel remains idle between the beginning of the slot and pCCATime later, so the node decrements its BC effectively pCCATime after the beginning of the CSMA/CA slot and transmits the packet to the medium at the end of the slot in which the BC reaches zero. Figure 5 shows the flow chart of the IEEE 802.15.6 CSMA/CA.

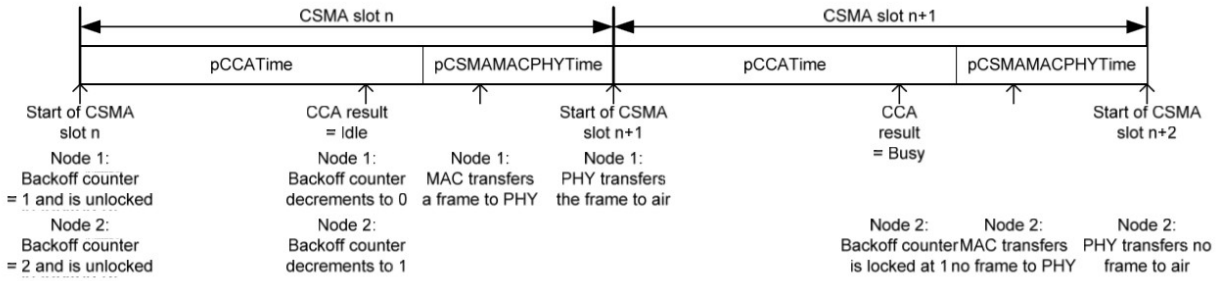

Figure 4: IEEE 802.15.6 CSMA slot structure

3.2 IEEE 802.15.6 performances evaluation models:

Several simulation studies have been conducted in the literature to analyze the IEEE 802.15.6 performances. Besides, efforts have been made in analytical modeling, which allowed better analysis of the overall characteristics of the standard without being limited to predefined scenarios like in simulation studies. As was the case for the earliest IEEE standards modeling, the proposed analytical

models for the IEEE 802.15.16 analyses were based mainly on Markov chain approaches and renewal reward processes and most of them have focused on random access protocols, such as the CSMA/CA and slotted ALOHA protocols. In the following section, we classify the analytical models to provide the IEEE 802.15.16 CSMA/CA performances according to the theoretical basis, using Markov chain or renewal reward processes.

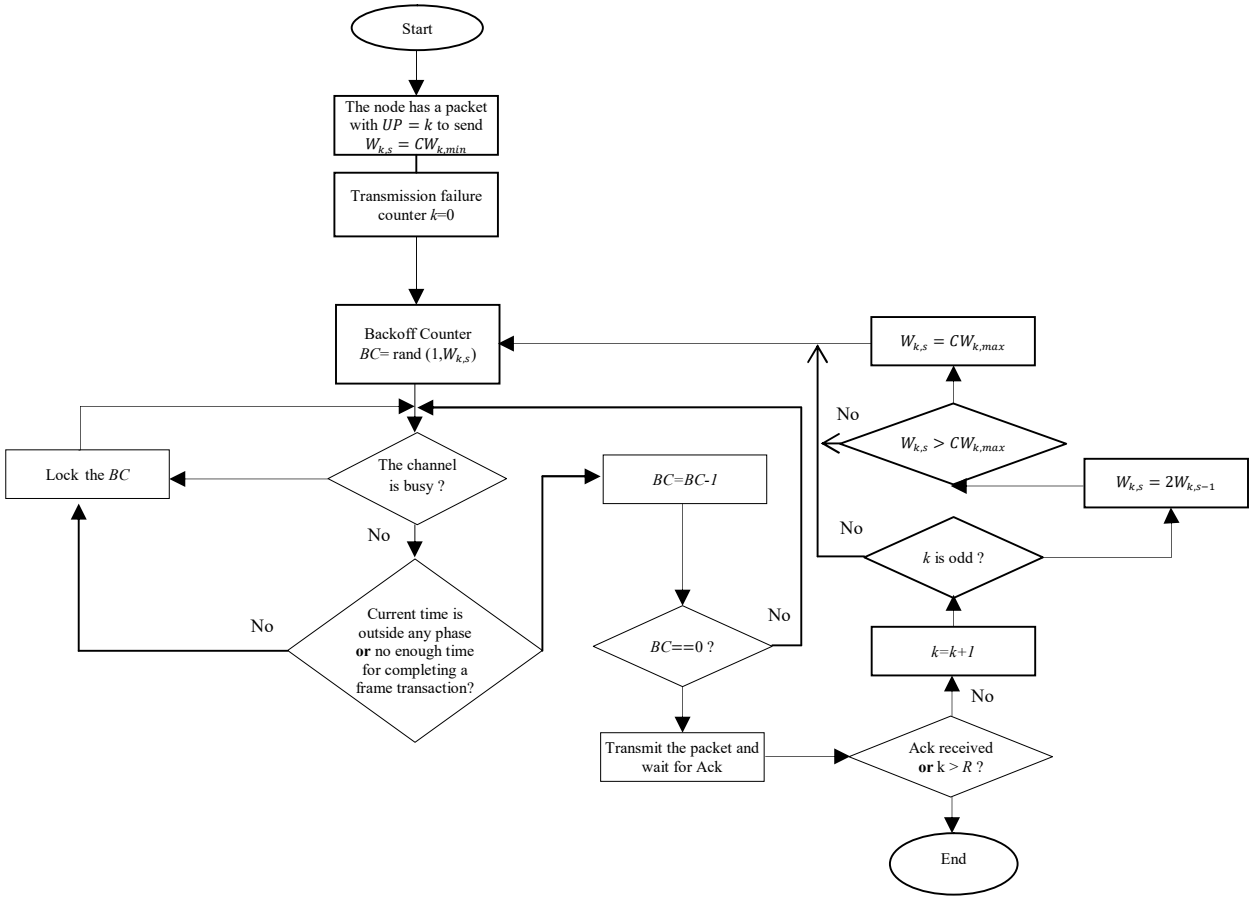

Figure 5: Data Transmission Flow Chart for CSMA/CA in IEEE 802.15.6

3.2.1 Markov Chain Based Analysis:

Markovian based analyses were widely used for performance evaluation of earlier IEEE standards, such as the IEEE 802.11 and the IEEE 802.15.4. These analyses were inspired by Bianchi's model, which used the Discrete-Time Markov Chain (DTMC) to analyze the throughput of the IEEE 802.11 Distributed Coordination Function (DCF) [47], [48]. S. Rashwand and al presented the first analytical models for performance analysis of the IEEE 802.15.6 CSMA/CA access scheme under different traffic regimes and channel states. They developed 4-dimensional DTMC combined with Probability Generating Functions (PGFs) for calculating the WBAN's metrics such as the mean

Backoff duration and the normalized throughput for all user priority nodes; [49] and [50] limited their studies to the EAP1 and the RAP1 access phases without presenting any queueing analysis of the node buffer. In [38], the authors extended their work to take into account EAP1, RAP1, EAP2, RAP2, and type-I/II access phases while in [8], the authors included to the proposed model a Geo/G/1 queueing sub-model of the node buffer. They showed that the channel was always utilized by high-priority sensor nodes due to their small Backoff durations and concluded that smaller and larger access periods affect the medium utilization. [9]constructed a DTMC that efficiently depicts the states of an IEEE 802. 15.6 CSMA/CA. Unlike the previous proposed analytical models, the time spent by a node while waiting for an acknowledgment (Ack) frame after sending a packet is taken into consideration in this model. In [12], a generalized analytical model for performance evaluation of the IEEE 802.15.6 CSMA/CA is proposed using a 3-dimensional DTMC with Backoff stage, Backoff counter and retransmission counter as stochastic parameters. The authors modeled the Backoff locking mechanism, which occurs due to insufficient remaining time in the Random Access Phase (RAP), by incorporating a dynamic time-variant variable into the proposed analytical model. To make simulation results similar to the practical performances, the authors considered a non-ideal channel by introducing Bit Error Rate (BER), multipath effect, shadowing standard deviation, and an error probability in the evaluation of the reliability, throughput, and energy consumption. Unlike the previous models that analyzed the CSMA/CA access scheme, the authors of [10] and [51] presented an analytical model to estimate the saturation throughput of the IEEE 802.15.6 prioritized Slotted Aloha access scheme under saturation regime and an ideal channel condition.

The Markov chain-based model was also used to analyze many improvements of the IEEE 802.15.6 standard. In [52] and [11], a DTMC is used to model a new Backoff procedure called Prioritized Fibonacci Backoff (PFB) for the IEEE 802.15.6 CSMA/CA under non-saturated conditions to predict the normalized throughput and the mean service time of the network. In [53], the authors proposed a new access mechanism by defining a new algorithm for dynamic Backoff bounds assignment, which takes into consideration the traffic state of the network after that they investigated the performance of an enhanced IEEE 802.15.6 CSMA/CA access mechanism by using the DTMC model. In [54], the authors proposed an adaptive superframe structure-based scheme for improving the reliability of emergency data. Based on DTMC, an analytical model has been developed to compute the reliability and the average delay experienced by emergency data frames. In [13], the authors proposed a sleep mechanism for the IEEE 802.15.6 CSMA/CA access scheme in a typical WBAN deployed in a

hospital environment. To analyze lifetime and delay requirements, the authors developed an analytical model based on PGFs and Markovian techniques. In [14], the authors proposed a new method to calculate the BER and Packet Error Rate (PER) and then analyzed the performance of WBANs while assuming a fluctuation of received Signal to Noise Ratio (SNR) of the BNC. They showed that the DTMC method used in previous work to calculate the access probability of all sensor nodes was not effective and complicated while considering the BER/PER. For this aim, they proposed the use of Markov Chain Monte Carlo (MCMC) method to calculate the access probability.

3.2.2 Renewal Reward Process-based Analysis:

The renewal reward process has been used for IEEE standards analyses in the same way as Markov based models. Initial work in this axis was made to provide analytical models for IEEE 802.11 based Wireless Local Area Networks (WLANs) analysis, where the authors of [55] extended the analysis of Bianchi's proposed Backoff model for the IEEE 802.11 DCF to unsaturated conditions by using the renewal reward theorem. From the fixed point analysis, the authors provided explicit formulas for the collision probability, the mean attempt rate, and the mean throughput. In [56], the authors provided an analytical model for the IEEE 802.15.4 MAC protocol. They modeled the IEEE 802.15.4 CSMA/CA behavior by a three-level renewal reward process and they used fixed-point techniques for solving the proposed model to obtain MAC layer metrics such as the throughput and the mean access delay. The authors in [15] presented a simple and accurate model to predict throughput, energy consumption, and transmission delay for different node priorities with the assumption of a finite number of nodes under the saturated regime and lossy channel conditions. The accuracy of the proposed model was validated by simulations. In Table 5, we summarize the main related work to our proposed approach.

We notice from the review that all the proposed analytical models assumed that IEEE 802.15.6 based WBANs are composed of sensor nodes that generate only one user priority type of traffic. As we mentioned in the introduction, this assumption cannot allow analyzing the standard performances in all possible scenarios, especially when sensor nodes have to generate at least two types of traffic with different user priorities. To cover such applications' scenarios, heterogeneous networks in terms of traffic's priority must be taken into account in the proposed analytical models of the IEEE 802.15.6 CSMA/CA access scheme.

	Access scheme	Assumptions	Analytical approach	Queueing	Access phases	Traffic
[49]	CSMA/CA	- Saturation condition - Noisy channel	DTMC	No	EAP1, RAP1	Each node has one UP traffic
[50]	CSMA/CA	- Saturation condition - Error-Prone Channel	DTMC	No	EAP1, RAP1	Each node has one UP traffic
[38]	CSMA/CA	- Saturation regime - Error prone channel	DTMC	No	EAP1, RAP1, EAP2, RAP2, and type-I/II	Each node has one UP traffic
[8]	CSMA/CA	- Non-saturated - Error-Prone Channel	DTMC	Geo/G/1	EAP1, RAP1, EAP2, RAP2, and type-I/II	Each node has one UP traffic
[9]	CSMA/CA	- Saturated - Non-ideal channel conditions	DTMC	No	RAP	Each node has one UP traffic
[10]	Slotted Aloha	- Non-Saturated - Ideal channel condition	DTMC	No	RAP	Each node has one UP traffic
[15]	CSMA/CA	- Saturated traffic conditions - Error-prone channel with	Renewal Reward approach	No	RAP	Each node has one UP traffic
Proposed approach	**CSMA/CA**	- **Saturation regime** - **Ideal channel condition**	**Renewal Reward approach**	**M/G/1 with non-preemptive priority**	**EAP1, RAP1**	**Heterogeneous traffic in term of priority**

Table 5: Comparison of analytical models proposed for IEEE 802.15.6 based WBANs.

3.3 Security paradigm in the IEEE 802.15.6 standard:

The IEEE 802.15.6 standard aims to provide strong security for sensitive information in medical applications. To that end, the standard provides complete security architecture as depicted in Figure 6, where a session refers to a period in which a PTK remains valid. The length of a session is determined by the security policy and is further limited by the technical restrictions on the reuse of the same PTK for successive messages. A secured frame is a frame which is secured by authenticity, integrity,

confidentiality, and replay protection[57]. The IEEE 802.15.6 standard operates in the following three security levels [58]:

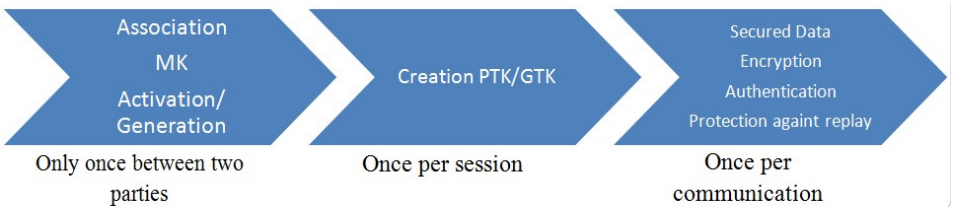

Figure 6: The structure of security in the IEEE 802.15.6 standard

Level 0: Unsecured communications. At this level, data is transmitted in unsecured frames that provide no mechanisms for integrity validation, authenticity, and defense of repetition, privacy, and confidentiality.

Level 1: Authentication but not encryption. At this level, data is transmitted in secured authenticated but unencrypted frames that provide mechanisms to validate integrity, authenticity, and defense against replay, and there is no protection of privacy and confidentiality.

Level 2: Authentication and encryption. This is the highest level of security in which data is transmitted in authenticated and encrypted frames. Therefore, the capability of providing mechanisms for integrity validation, authenticity, defense against replay, privacy, and confidentiality.

A security association as defined by the IEEE 802.15.6 standard is a level 2 security procedure that identifies a node at the BNC's level. It is the first step in establishing a secure connection. It is done by activating a pre-shared MK or generating a new one. Once the MK is validated, the pair generates in a unicast communication a PTK that will be used only once per session, while in multicast communication, a Group Time Key (GTK) is generated and shared with the entire corresponding group [58]. In both cases, the standard provides for the use of encryption equivalent to AES-128 (Advanced Encryption Standard).

In the standard's security level 2, a node that connects to a network goes through the following stages:

- **Orphan**: Is the initial state where the node has no relationship with the BNC. Node and BNC cannot switch to the associated state if they fail to validate a shared MK key.
- **Associated**: To get to this state, the node must validate the pre-shared MK. The node and the BNC are allowed to exchange frames with each other to confirm ownership of this shared MK,

create a PTK, and switch to the secure state. If the MK is invalid or missing during the creation of the PTK, it will return to the Orphan state.

- **Secured**: The node switches to this state after creating a PTK. The node and the BNC can exchange security dissociation frames, secure connection allocation frames, a connection request, and non-secured control frames.

- **Connected**: The secure node can exchange requests and connection assignment frames with the BNC to form a connection and switch to the connected state. The node and the BNC are not allowed to send unsecured frames to each other, except for unsecured control frames if authentication of control type frames has not been selected during association.

The diagram of the security states of the sensors in the IEEE 802.15.6 standard is shown in Figure 7.

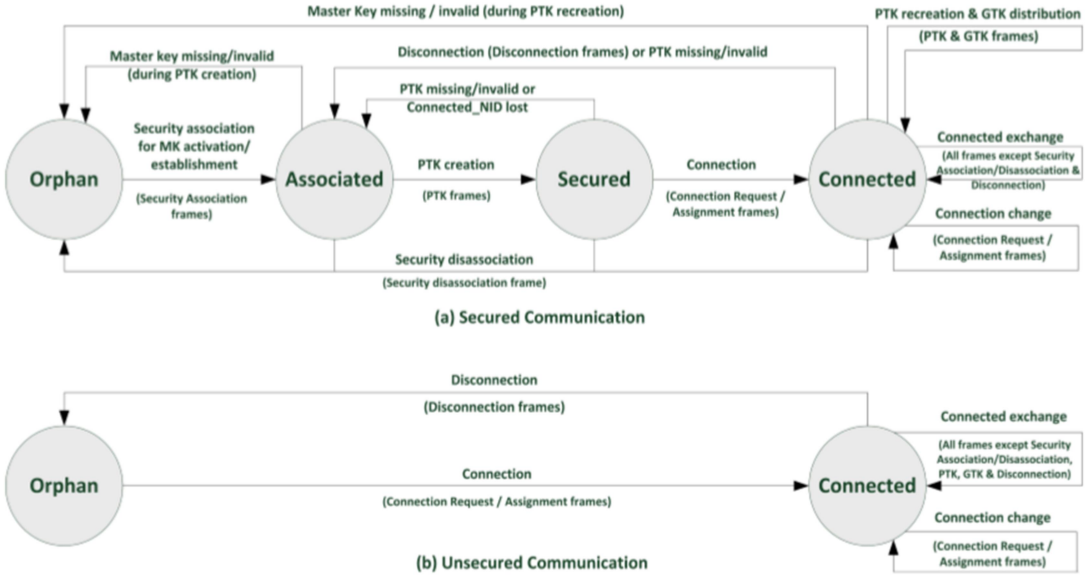

Figure 7: Security status diagrams in the IEEE 802.15.6 standard

3.3.1 Association protocols:

The transition between the above states is performed through the security association, the PTK creation procedures, and the security disassociation. The IEEE 802.15.6 standard includes five protocols for the security association (one for activating a pre-shared MK and four for establishing a new shared MK), one protocol for the PTK creation, and one protocol for the security disassociation[5].

The five protocols are very similar, and they vary little in details and requirements, so in what follows, we only detail the first protocol's procedure (Protocol II), which is used to agree with a new pre-shared MK, we will then give the differences with the others protocols.

THE ASSOCIATION PROTOCOL "PROTOCOL II":

Initially, the sensor node and the BNC generate a Secret Key (SK), from which a Public Key (PK) is derived. Using the elliptic curve cryptography (Diffie-Hellman algorithm) the MK will be generated after the following steps.

- The security association is initiated by the sensor node(A) by sending Security Association frame to the BNC (B) in the following form:

$$A \rightarrow B : \{ IDB|||IDA|||SSS||AC|||NA||PKAX|||PKAY||XX\} \quad (2)$$

- Upon receiving the first Security Association frame, the BNC responds to the node by the second Security Association frame:

$$B \rightarrow A : \{ IDA|||IDB||SSS||AC|||NB||PKBX|||PKBY||XX\} \quad (3)$$

Where, (PKAX, PKAY) denote the x and y coordinates of PKA, the ID represents the identifiers of the network element, SSS (Security Suite Selector) refers to cryptographic algorithms and key verification and generation protocols (I to V). N and AC are variables used in the different algorithms and XX is an optional field.

After that, the two parties start to the generation of temporary verification variables (T2 and T3 for A, and T'2 and T'3 for B), calculated according to the algorithms agreed upon in the SSS variable (DHKey, RMB_128 (DHKey)), and exchange them back:

$$B \rightarrow A: \{IDA|||IDB||SSS||AC|||NB||PKBX|||PKBY|T'2\} \quad (4)$$

$$A \rightarrow B:\{ IDB|||IDA|||SSS|AC|||NA||PKAX|||PKAY||T3\} \quad (5)$$

The comparison of the variables calculated internally with those sent by the other party determines the validation of the connection and allows the generation of a new shared MK using the Cipher-based Message Authentication Code algorithm (CMAC)[5]. We summarized the other association protocols differences in the following table (Table6) as follows[59]:

Protocol	Requirement
Protocol I	The node and the BNC have pre-shared MK, which can be activated through this protocol.
Protocol II	No authentication and no special requirements.
Protocol III	Requires the transfer of a pre-shared public key from a node to the BNC over an out-of-band channel. Then the BNC must register the public keys of the nodes.
Protocol IV	Requires that a node and a BNC pre-share a password (PW). The node sends a hidden public key in which the PW is a positive integer, converted from the pre-shared PW between the node and the BNC. Thus, the field $PK'_{AX}=PK_{AX}-PW_X$ and $PK'_{AY} = PK_{AY}-PW_Y$.
Protocol V	Requires that the node and BNC each have a display that shows a decimal number. Before accepting a new MK, a human user must verify that the two displays are identical.

Table6: Differences in association protocols of the IEEE 802.15.6 standard

3.3.2 Security Protocol vulnerabilities:

In the IEEE 802.15.6 standard, public keys are not always accompanied by digital certificates because the sensor nodes are severely limited in resources, and therefore cannot always store certificates or perform their validation. Nevertheless, there are certain types of extra-resourced sensors that can support the deployment of security certificates [14].In the absence of such mechanisms, the above-mentioned association protocols can be vulnerable to several types of attacks shown in Table7 [10], [59] and [57].

Protocol	Vulnerability	Types of attacks
Protocol I	does not include any secret information	/
Protocol II	Un-authenticated and unencrypted key exchange in the protocol.	• The impersonation attack. • KCI attack.
Protocol III	The exchange protocol for one of the keys not authenticated and not encrypted, but pre-shared for the other.	• KCI attack.

Protocol IV	An un-authenticated and unencrypted key exchange in the protocol, but protected by a password.	• The impersonation attack • KCI attack. • Offline Dictionary attacks.
Protocol V	An un-authenticated and unencrypted key exchange in the protocol.	• The impersonation attack. • KCI attack.

Table7: Association protocols vulnerabilities.

Because of the various flaws and vulnerabilities observed in the association protocols, where the primary exchanges are done in clear, it becomes necessary to find a solution. It is therefore intending to protect communications from the beginning of exchanges between sensor nodes and the BNC that the solution presented in chapter seven (7) is proposed.

3.4 Conclusion

In this chapter, we presented the IEEE 802.15.6 standard and the related CSMA/CA access scheme. An overview of the literature work dealing with the III 802.15.6 performance evaluation is presented. We classified the analytical models providing the IEEE 802.15.16 CSMA/CA performances according to their theoretical basis (Markov chain or renewal reward process).Finally, we presented a security paradigm proposed by the IEEE 802.15.6 standard and its identified vulnerabilities.

4 PERFORMANCE EVALUATION OF IEEE 802.15.6 MAC IN MONITORING OF A CARDIAC PATIENT

In this chapter, we evaluate and compare two wireless IEEE standards; IEEE 802.15.6 and IEEE 802.15.4 over realistic requirements and constraints of home monitoring of an individual cardiac patient. The goal of this evaluation is to show which of these two standards more fills the requirements of this type of application. We will concentrate our study on the EAP and RAP phases which use the CSMA/CA access schemes with priority, because it is the most important contribution of the IEEE 802.15.6 comparing to earlier IEEE wireless standards. The ISO/IEEE 11073 Draft for Point-of-Care (PoC) medical devices [60] is a standard that addresses the use of radiofrequency wireless technology for the transport of medical data both to and from PoC medical devices. This standard defines many medical use cases representing a board of typical healthcare scenarios ranging in degree of criticality and potential wireless complexity. These specific use cases are defined to estimate, compare, and contrast performances of wireless technologies in terms of throughput, latency, data rate, and many other parameters. For our evaluation of the IEEE 802.11.6 standard, we will utilize the Use Case of home monitoring of an individual cardiac patient (UC1a) as a simulation scenario, which is defined as follows:

An individual patient has been sent home following recovery from cardiac surgery and is ambulatory but remains within the confines of his home, with perimeter dimensions 17m x 9m, physiologic parameters monitored from a wireless Patient Worn Device (PWD) include continued 3-lead ECG (three electrodes) as well as scheduled episodic Blood Pressure (BP) and Heart Rate (HR), blood oxygen saturation (SpO2) values are sent episodically from a fingertip monitor to the PWD. There is a priority real-time alarm that is transmitted one way from the PWD if an arrhythmia is detected and is directly sent to the nurse at the central surveillance station at the local hospital. Table 8 presents the data transport requirement for the selected scenario [61].

Device	Data Category	transmission interval (ms)	Throughput (Kb/s)	Max end-to-end latency (ms)	Min range (m)
PWD (BNC)	Uplink	Periodic	2	10 000 (to the hospital)	17
Fingertip monitor	SpO2	2000	0.1 per sample	< 200 (to PWD)	1
Three Electrodes	1 ECG vector HR	40	1.250+0.1 for alarm	< 100 (to PWD)	1
BP monitor	BP	2000	0.1 per sample	< 100 (to PWD)	1

Table 8: Data transport requirements for a home cardiac patient [60].

4.2 **Simulation parameters:**

To perform simulations, we chose the Castalia open-source simulator [62] designed for networks of low-power embedded devices, that offers a node behavior simulation in realistic wireless channels and radio models. All simulations described in this chapter are realized with Castalia 3.2.

As described in Figure 8, the WBAN considered in our simulations incorporates five (5) sensor nodes and one BNC. To ensure the 3-lead ECG supervision, three (3) electrodes are deployed on the rib cage of the patient. The two other sensors are placed on the left and right arms to measure the SpO2 and blood pressure, respectively. All these sensor nodes communicate wirelessly with the BNC. Due to the emergency aspect of the ECG electrodes data, we will assign them the highest user priority (UP=7) and for the other sensors nodes, we attribute an ordinary user priority (UP=5).

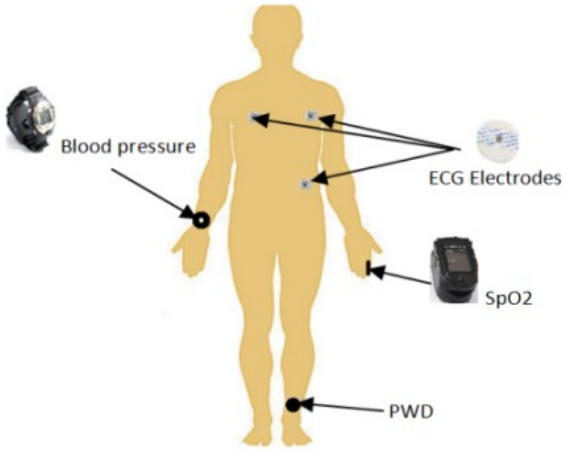

Figure 8: Simulated Network Topology

In the first step of our evaluation, we will compare the performances of the IEEE 802.15.6 and IEEE 802.15.4 standards. After that, we will evaluate the IEEE 802.15.6 performances by varying many parameters. We start by varying the UP of one electrode node from the lower user priority (UP=0) to the highest one (UP=7) to show the effects of the UP value on the IEEE 802.15.6 CSMA/CA access scheme. Then we will vary the EAP and RAP phases' lengths to show their impact on the overall performances of the standard and the effectiveness of the use of the EAP access phase in this type of application.

In this evaluation, we used two different radios to meet the characteristics of each standard. The first radio meets with the IEEE 802.15.6 radio proposal [5] and the second one is the 2.4 GHz IEEE 802.15.4 RF Transceiver (CC2420) [63], which is used to evaluate the IEEE 802.15.4 standard. In all simulations, it is assumed that if the radio unit is not transmitting, it is either receiving or listening. Table 9 gives the various parameters defined for the two types of radio.

Parameters	IEEE IEEE802.15.6	IEEE 802.15.4 (CC2420)
Data rate (kbps)	1024	250
Modulation Type	DIFFQPSK	PSK
Bits Per Symbol	2	4
Bandwidth (MHz)	20	20
Noise Bandwidth (MHz)	1000	194
Noise Floor (dBm)	-104	-100
Sensitivity (dBm)	-87	-95
Power Consumed on reception mode (mW)	3.1	62
transmission power (dBm)	-15	-15
Power Consumed on transmission mode (mW)	2.93	32.67
Power consumed on transition (transmission, reception) (mW)	3	62
Time of transition (transmission, reception)	0.02	001

Table 9: Simulation Radio parameters

In addition to the previous parameters, we took some default simulations parameters proposed by Castalia (slot length, Mac buffer size, etc.). The remaining parameters used in our simulations are listed in Table 10.

Parameters	IEEE 802.15.6	IEEE 802.15.4
Access scheme	CSMA/CA (with priority)	Slotted CSMA/CA
Simulation time (second)	51 (200 repetition)	
Slot allocation length (ms)	10	15.36
MAC Buffer size	32 packets	32 packets
Retransmission packets tries	2	2

PHY Layer overhead (Bytes)	6	6
Mac frame overhead (Bytes)	7	14
Packet header overhead (Bytes)	05	05
Data payload (Bytes)	100	100
Packet rate (packet/s)	Nodes (1, 5) = 0.5, Nodes (2,3,4) = 25	
Priority	Nodes (1, 5) = 5, Nodes (2,3,4) = 7	
Number of EAP Slots allocation	1 (RAP length= 32- EAP length)	

Table 10: Simulation parameters

4.3 Performance evaluation and results:

The performance metrics considered in this chapter are: the mean packet delivery rate, the mean consumed energy, and the mean packet latency. The mean packet delivery rate per node is defined as the number of successfully received packets by the BNC divided by the number of transmitted packets by all WBANs nodes, while the mean packet latency refers to the interval between the packet arriving at the local MAC layer and the successful data reception by the BNC.

a- Energy consumption:

The consumed energy histogram presented in Figure 9 shows the average consumed energy per node for the two standards where the EAP phase length is set to 16 slots for the IEEE 802.15.6 standard.

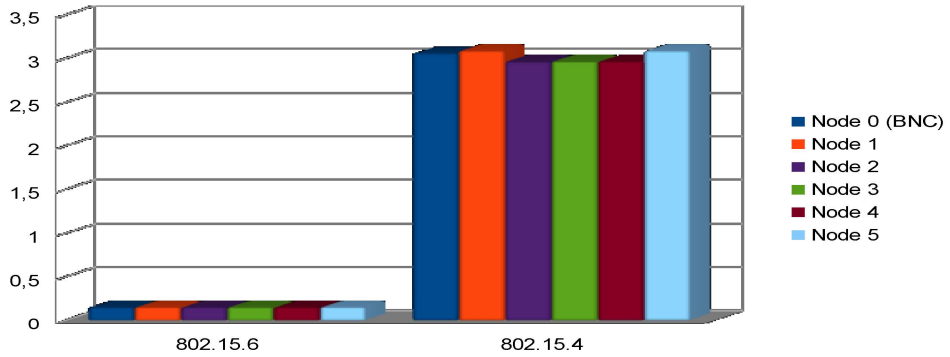

Figure 9: Consumed energy per node in joules

We notice from Figure 9 that the consumed energy in the IEEE 802.15.6 is less than the consumed one in the IEEE 802.15.4. This is due mainly to the type of the radio transceiver used by each standard. As shown in Table 9, the consumed power in reception and transmission modes is greater for the IEEE 802.15.4 radio unit than the IEEE 802.15.6 one. The second point to notice is that the amount of the consumed energy by ECG electrodes (2, 3, and 4) is lower than the amount consumed by SpO2 and BP sensor nodes. This is due to the packet generating rate, where the ECG nodes generate 25 p/s while the

other nodes generate only 0,5 p/s. As known the more the transmitting time increases the more the reception/listening time decreases. This fact affects the amount of energy consumption because reception/listening consume more than transmitting as shown in Table 9.

b- Latency:

Figure 10 shows the mean latency of the received packets at the BNC (node 0). We notice that most of packets are received with latency less than 25 m/s in the IEEE 802.15.6 standard, where in IEEE 802.15.4 standard most packets are received with latency superior to 200 m/s. This result is explained by the access schemes used by the two standards at the MAC layer. The ECG electrodes have the greatest packet generating rate according to the ISO/IEEE 11073 guide. Thus, by using the IEEE 802.15.6 CSMA/CA with priority, these nodes will be assigned the highest UP value, resulting in small contention windows, which allows the ECG nodes to send their data with a minimum waiting delay. However, in the slotted CSMA/CA used by the IEEE 802.15.4 standard, all nodes have the same probability to access the medium. This will increase the collision probability and result in a high delay. On the other side, the high data rate offered by the IEEE 802.15.6 at the physical layer justifies more these results.

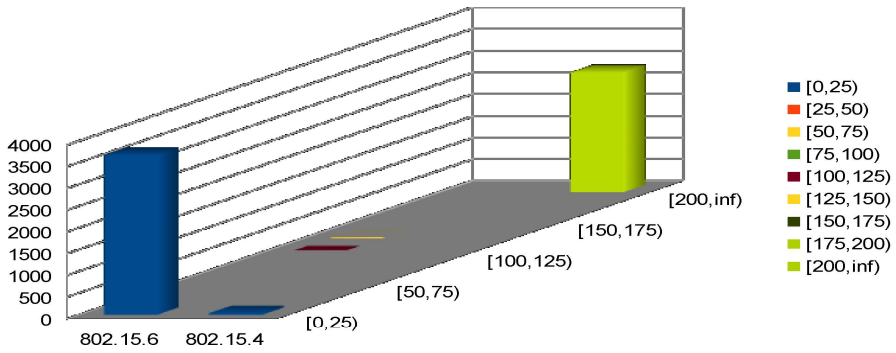

Figure 10: Latency intervals (ms) of IEEE 802.15.6 and the IEEE 802.15.4

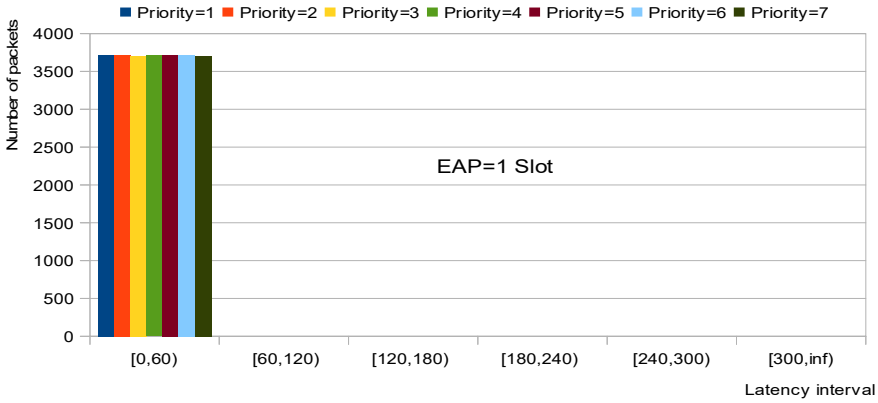

Figure 11: Latency intervals (ms) of IEEE 802.15.6 with EAP=1 Slot

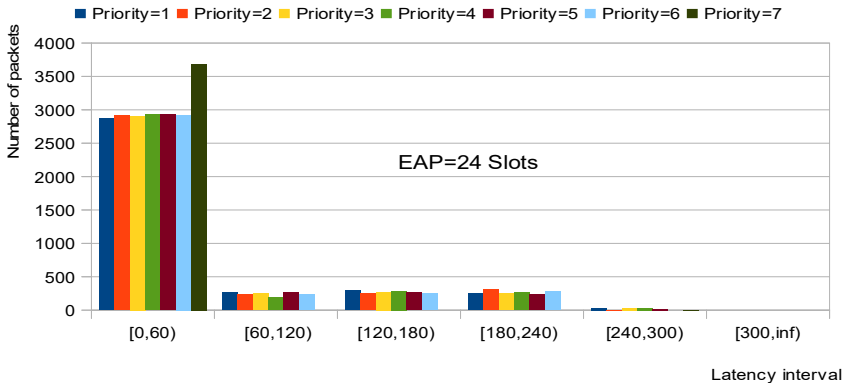

Figure 12: Latency intervals (ms) of IEEE 802.15.6 with EAP=24 Slots

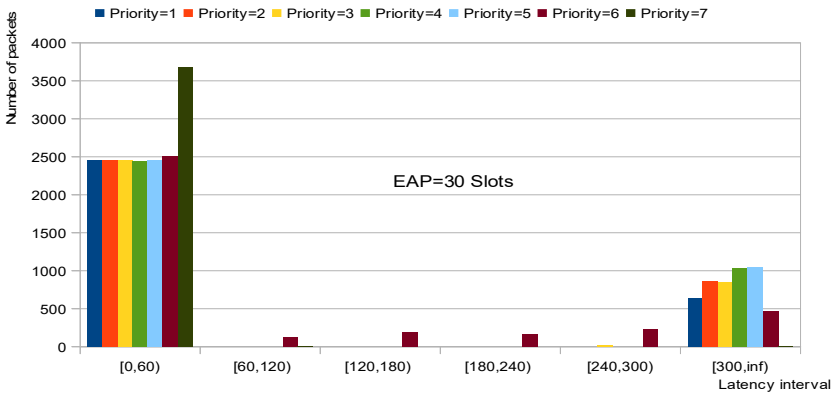

Figure 13: Latency intervals (ms) of IEEE 802.15.6 with EAP=30 Slots

In a second step, we evaluated the influence of UP values on the latency while varying the EAP phase length. For this aim, we vary the UP values of an ECG electrode (node 3) from one (1) to seven (7). Figure 11, 12 and 13 show the latency of the received packets with an EAP length equal to one (1), twenty-four (24), and thirty (30) slots respectively. From Figure 11, we can notice that with an

EAP length equal to 1, all packets are received with a latency inferior to 60 ms. However, with an EAP length equal to 24 and 30 slots, only packets with the highest (UP = 7) are received with a latency inferior to 60 ms, while the packets with UPs different from 7 will have higher latency. This is due essentially to the role of each access phase. The EAP is reserved only to emergency packets with high priority while the RAP is used for emergency and non-emergency transmission. Accordingly, all non-emergency packets generated during the EAP phase will be buffered until the start of the RAP phase. This buffering delay will increase the latency of these packets.

c- Packet delivery rate:

The Packet Delivery Rate (PDR) histogram presented in Figure 14 shows the average PDR per node for the two standards. We notice that the rate of successfully received packets by the BNC in the IEEE 802.15.6 standard is higher than the IEEE 802.15.4 standard. To explain this difference, we will give details on packets failure and their origin in Figure 15 and Figure 16 corresponding to the IEEE 802.15.4 and IEEE 802.15.6 respectively. We recorded the packet breakdown at the MAC layer of the senders. Then, we have classified them into five categories: a) Failed, buffer overflow (i.e., the packet was deleted because the MAC buffer was full). b) Failed, no Ack (i.e. a packet was transmitted to the radio without receiving the Ack), c) Failed, channel busy (i.e., packet failed because the CSMA mechanism never found the channel free, in all transmission attempts), d) Success, first try (i.e., an Ack was received on the first transmission attempt), e) Success, 2 or more tries (i.e., an Ack was received after more than one transmission attempt).

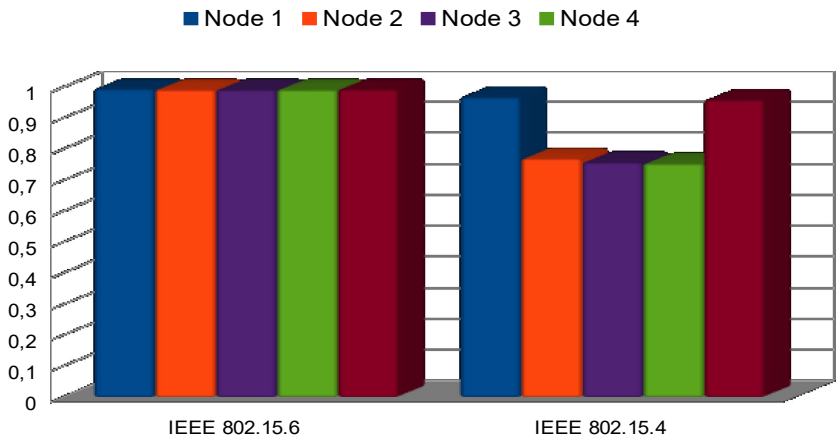

Figure 14: Packet delivery rate of 802.15.6 and 802.15.4

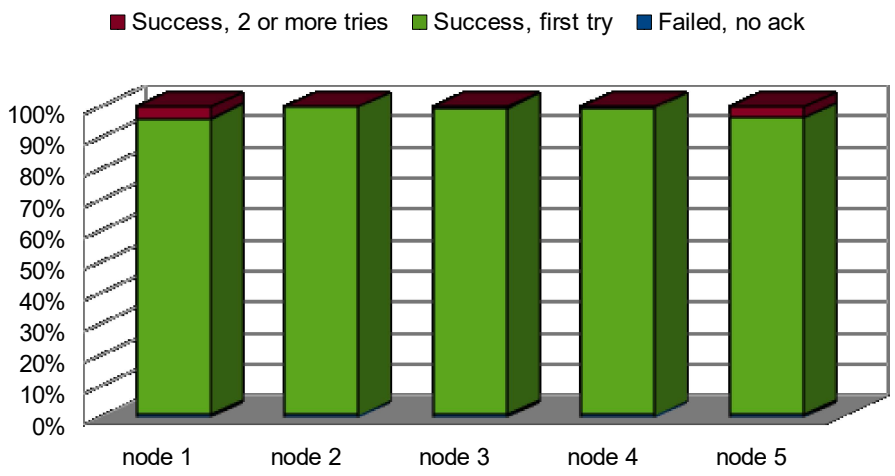

Figure 15: Data packets breakdown at the MAC layer for IEEE 802.15.4

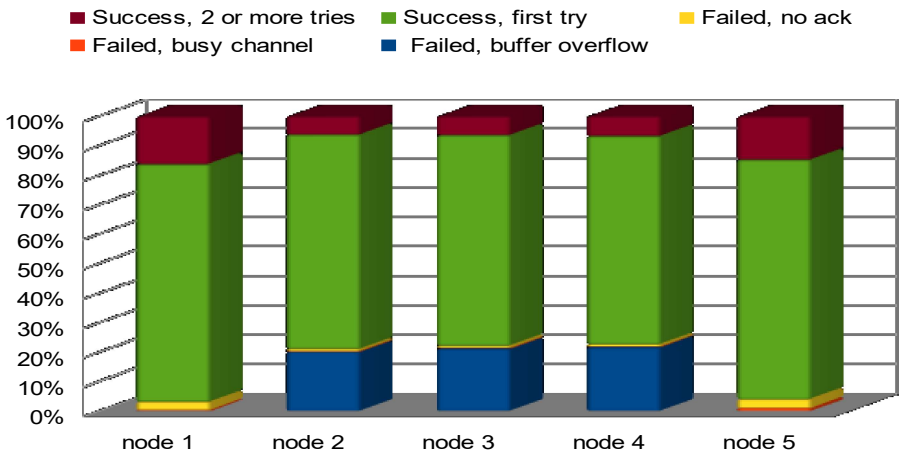

Figure 16: Data packets breakdown at the MAC layer for IEEE 802.15.6

Figure 15 and Figure 16 show the data packets breakdown per node for each standard. The results are shown in percentages. The important characteristic we notice is related to the increase of packets failure caused by the buffer overflow for nodes 2, 3, and 4, where it is zero for the other nodes. This is explained by the inability of the used radio transceiver and the Mac access scheme (IEEE 802.15.4 CSMA/CA) to satisfy the high sending data rate of the ECG electrodes (node 2, node 3, and node 4). As we know, the CC2420 radio used by the IEEE 802.15.4 cannot send up to 250 kb/s unlike the radio used by IEEE 802.15.6 which can reach the 10 Mb/s. thus, all nodes attempt to get access the medium to send their packets and put all new arriving packets in the buffers waiting for their turn to be sent. But, when a buffer reaches its maximum size, the arriving packets will be deleted. On the other hand, the same nodes do not suffer from this problem in the IEEE 802.15.6. This is due to the priority scheme used in the Mac layer and radio characteristics as explained above.

To evaluate the effect of UPs on packets breakdown at the MAC layer for IEEE 802.15.6, we varied the UP value of the node three (3) from one (1) to seven (7) and we showed its effect on the simulation results. The Figure 17 shows that the UP value has an important impact in the amount of packets failure. Having high UP value increases the reception probability of the packets on the first sending attempt. However, decreasing the value of this priority will increase the waiting time for their sent; therefore the number of failed packets will be increased due to the buffer overflows.

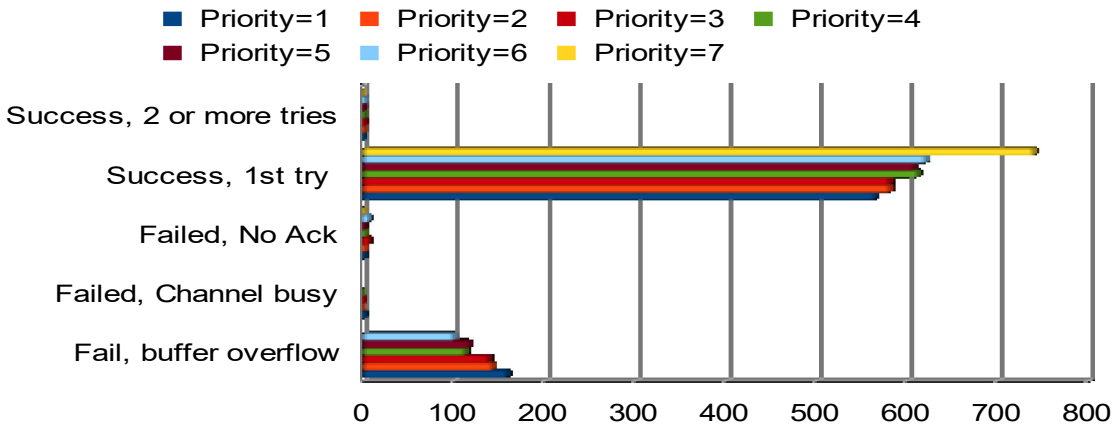

Figure 17: Data packets breakdown at the MAC layer for IEEE 802.15.6 where varying UPs

4.4 **Conclusion**

In this chapter, we have evaluated the performances of the IEEE 802.15.6 in terms of energy consumption, latency, packets delivery rate, and packets breakdown at the MAC layer while satisfying the ISO/IEEE 11073 requirements. In addition, to the energy efficiency, we have shown the effectiveness of the IEEE 802.15.6 in-home monitoring of an individual cardiac patient. Unlike the IEEE 802.15.4 standard, the IEEE 802.15.6 standard satisfies all the requirements of the ISO/IEEE 11073 guide. We also demonstrated that the use of UPs mechanism for the IEEE 802.15.6 CSMA/CA has a big influence on the network's performance; it guarantees timely service for higher UPs while decreasing the performance of lower UPs nodes.

5 QUEUEING MODELS EVALUATION WITH THE IEEE 802.15.6 STANDARD

WBAN is one of the emerging technologies that has the potential to significantly improve healthcare delivery, diagnostic monitoring, disease-tracking, and related medical procedures. However, QoS and reliability of successful communication must be handled to preserves patient life in critical situations. The standard IEEE 802.15.6 offers physical layers and a medium access control layer to ensure high reliability and timely transmission of emergency packets. By packets prioritization, the standard assigns the high user priority to emergency traffic and allows a dedicated EAP phase in the super-frame that authorizes the transmission of only high priority packets. As we showed in the chapter 2, the most of works treating the queueing in the IEEE 802.15.6 standard suppose that each node handles only one type of data, which is not valid in realistic scenarios. In many applications, WBANs incorporate nodes that sense different vital signs with different user priorities. In such cases, nodes must send their packets and eventually node's events report to the BNC. Without adequate queueing and scheduling strategies to send high priority packets first, the standard will not ensure a timely notifying of high emergency crisis to the hospital center.

In this chapter, we will propose an adapted LLQ to improve the QoS in WBANs using the IEEE 802.15.6 standard. LLQ system is composed of one priority queue and many low priority queues. Packets in low priority queues are scheduled only when there are no packets in the priority queue. To show the benefits of our proposed queueing strategy, we will evaluate the standard throw three queueing strategies; a) single FIFO head of line queue for all packets with length equal to 30 packets. b) two FIFO queues, one for emergency packets (UP=7) with length equal to ten packets and the second for the rest of packets (UP=0...6) with length equal to twenty packets. c) Our proposed LLQ with one high priority FIFO queue for emergency packets with length equal to nine packets and three waited FIFO queues using Class-Based Weighted Fair Queueing (CBWFQ) for the rest of the packets with lengths equal to seven packets for each of them[64]. The detail of our proposed LLQ with the weighted low priority queue is described in Figure 18.

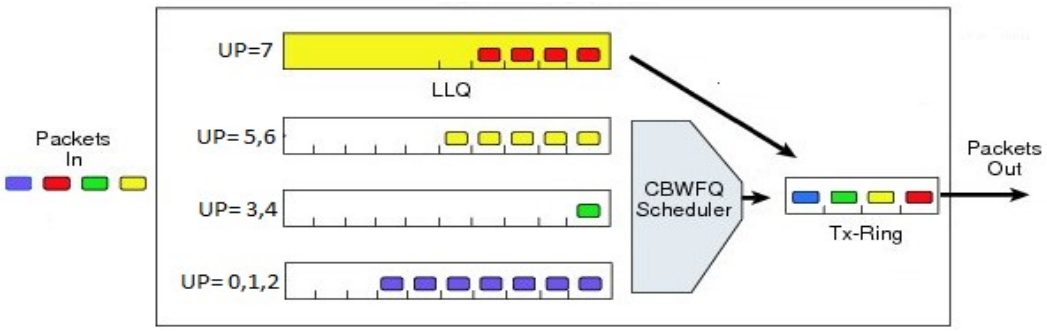

Figure 18: LOW LATENCY QUEUEING IN IEEE 802.15.6

5.2 Simulation parameters:

In this section, we evaluate the QoS of the standard IEEE 802.15.6 over realistic requirements and constraints of the home monitoring of an individual cardiac patient as described in section 4.2. The goal of this evaluation is to show the effectiveness of our queueing strategy to fulfill the requirements of this standard. We have used the same radio parameters as described in chapter 4 (Table 9). The rest of the simulation parameters are described in the following table.

IEEE 802.15.6 simulation parameters	
Simulation time (second)	51 (50 repetition)
Slot allocation length (ms)	10
Retransmission packets retry	2
Phy Layer overhead (Bytes)	6
Mac frame overhead (Bytes)	7
Packet header overhead (Bytes)	05
Data payload (Bytes)	100

Table 11: IEEE 802.15.6 Simulation parameters

In all simulations, we supposed that the WBAN operates under saturation conditions while the arrival packets follow a Poisson Process with lambda equal to 50 p/s. The whole queues size equal to thirty packets. We fixed weights for the LLQ with three low priority queues as fellow: weight=3 for packets with UP=5, 6.weight=2 for packets with UP=3, 4. weight=1 for packets with UP=0, 1, and 2.

We carried out many simulations while varying the percentage of emergency packets (UP=7): (100%, 50% … 15%). For example: 15% of emergency packets mean that 85% of packets are with user priority vary uniformly between 0 and 6.

5.3 Performance Evaluation and results:

The performance metrics, considered in this evaluation, are: the PDR, consumed energy, and average packet latency. To evaluate the behavior of the standard while handling emergency packets using different queueing strategies, we considered in simulations that the superframe is composed of only EAP and RAP phases. We have fixed the length of the EAP phase length to 128 slots and 127 for the RAP phase.

a. Packet delivery rate:

The PDR histograms presented in Figure 19, Figure 20, and Figure 21 show the average packet delivery rate for each of the three queueing strategies. We notice that the rate of successfully received packets by the BNC while using two queues or LLQ is higher than while using one queue. This is explained by the number of dropped packets due to the buffer overflow. During the EAP phase, when only one queue is used the packets sent will be blocked if there is a non-emergency packet at the head of the queue. In such a case, all newly arriving packets will be deleted after reaching the maximum size of the queue. The second point that we noticed from these figures is that the number of delivered packets decrease while decreasing the percentage of high emergency packets. This is explained by the high transmission rate and the low buffering time of high emergency packets. The sent time of a packet depends on the Backoff duration and the transmission time and as we know the Backoff duration of emergency packets is less than the Backoff duration of low non-emergency packets. The third concluded remark concerns the reception rate of non-emergency packets; while using two queues, all non-emergency packets have the same reception rate whereas in the LLQ we have a clear amelioration of the reception rate of packets with user priority equal to six and five to the detriment of low priority packets (UP=0, 1 and 2). This is due mainly to the weights set in our simulation which promote these packets.

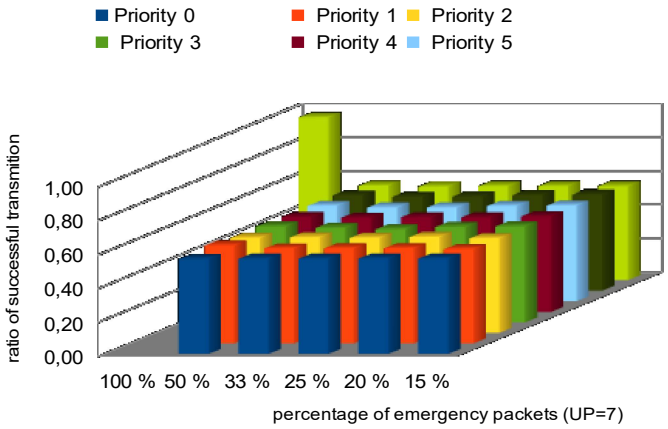

Figure 20: Packet delivery rate of IEEE 802.15.6 for one queue strategy

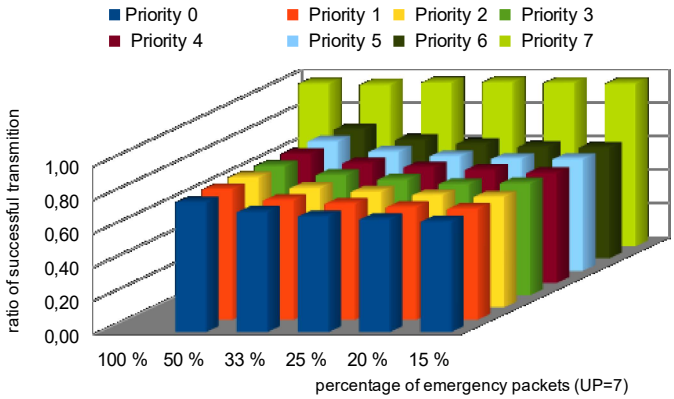

Figure 19: Packet delivery rate of IEEE 802.15.6 for two queues strategy

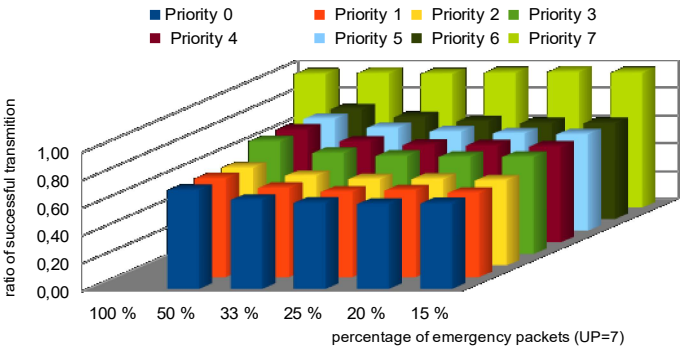

Figure 21: Packet delivery rate of IEEE 802.15.6 for LLQ strategy

To explain the differences in packet delivery rates, we will give details of packets failure and their causes in Figure 22 Figure 23, Figure 24 corresponding to one queue, two queues, and LLQ with weighted queues respectively, by recording the packet breakdown at the MAC layer of the senders.

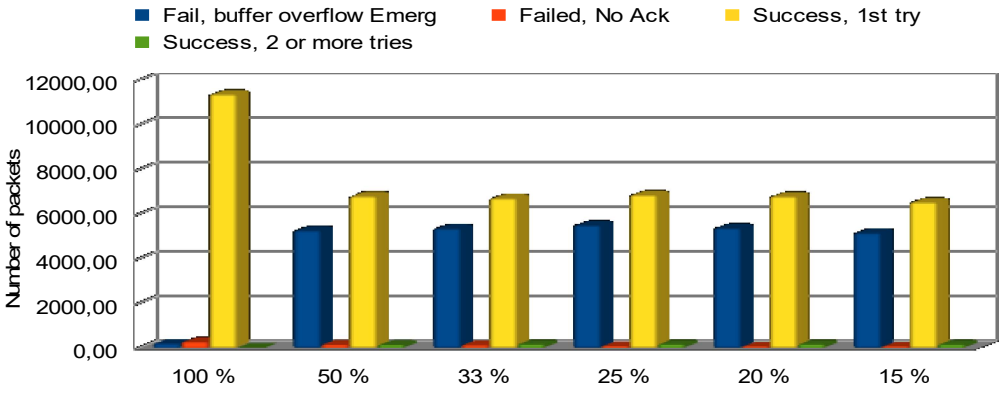

Figure 22: Data packets breakdown at the MAC for one queue strategy

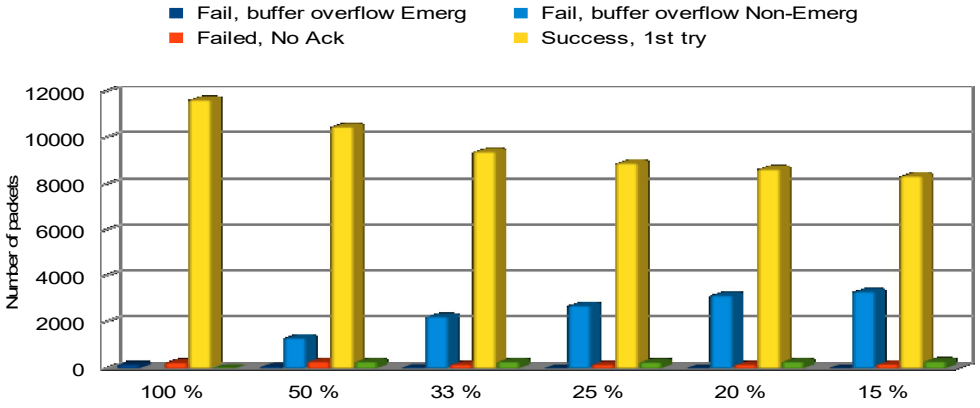

Figure 23:Data packets breakdown at the MAC for two queues strategy

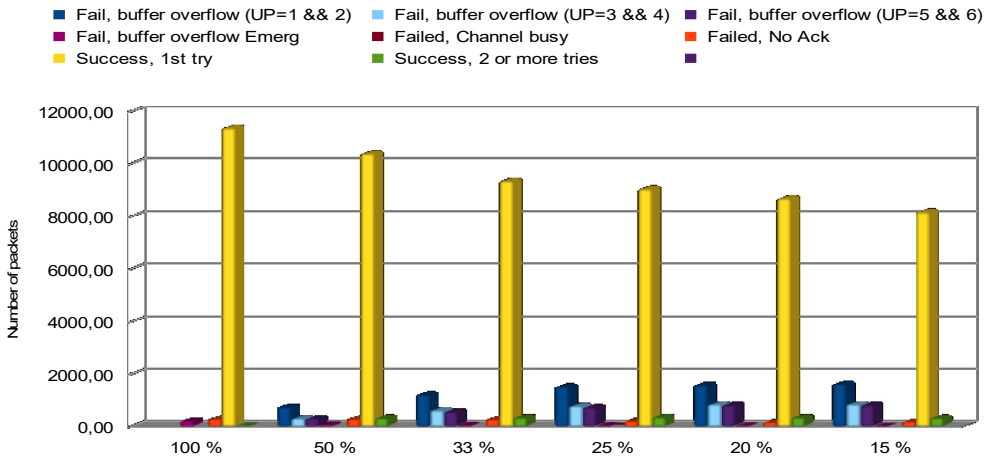

Figure 24:Data packets breakdown at the MAC for LLQ strategy

The results in Figure 22, Figure 23, and Figure 24 are shown in number of packets. The first important characteristic that we noticed from these figures is that the main cause of transmission failure of packets is the buffer overflow, which is mainly related to the queueing and the scheduling strategy. All arriving packets will be buffered in queues, and wait their turn to be sent. When a queue reaches its maximum size, all the new arriving packets will be deleted. Secondly, from Figure 22, we remark a high number of packets failure of all types of packets including the high emergency ones. As we explained above, the one queue strategy causes a high dropping of all types of packets by the buffer overflow because the packets arrival rate is higher than the transmission rate blocked by low priority packets. Figure 23 and Figure 24 illustrating the two queues and the LLQ strategies, show that the packet's failure is influenced by the weight of each queue and that the high emergency packets failure is almost null comparing to non-emergency packets. This is due to the high priority queue reserved for the emergency packets in these strategies.

b. Latency:

Figure 25 shows the average latency of all received packets by the BNC for each of the three queueing strategies. We noticed that the LLQ strategy offers the lowest average latency and the one queue strategy the highest average latency. This is explained by the user priorities of transmitted packets, as we mentioned above the Backoff time decrease while increasing the user priority. LLQ with weighted queues strategy gives an exclusive priority for high emergency packets and it decreases the probability of serving low priority packets according to the weight of the queue. On the other hand, in tow queues strategy, emergency packets are served fistly, after that the rest of packets are served according to their arriving times. In the one queue strategy, all packets are served according to their arriving times without giving any advantage for emergency packets. Besides, in one queue strategy, non-emergency packets will block packets sending during the EAP phase which results in high buffering time and therefore a high latency.

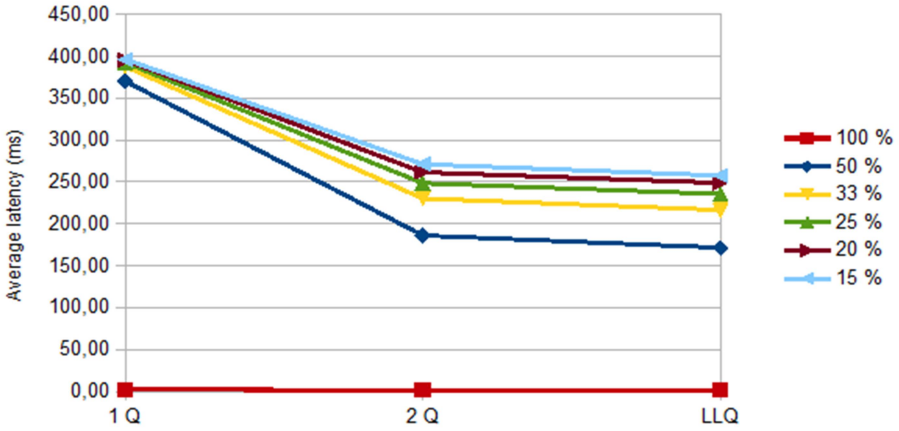

Figure 25: The average latency for one queue, two queues, and LLQ strategies

More detail on the latency of emergency packets is given in Figure 26.

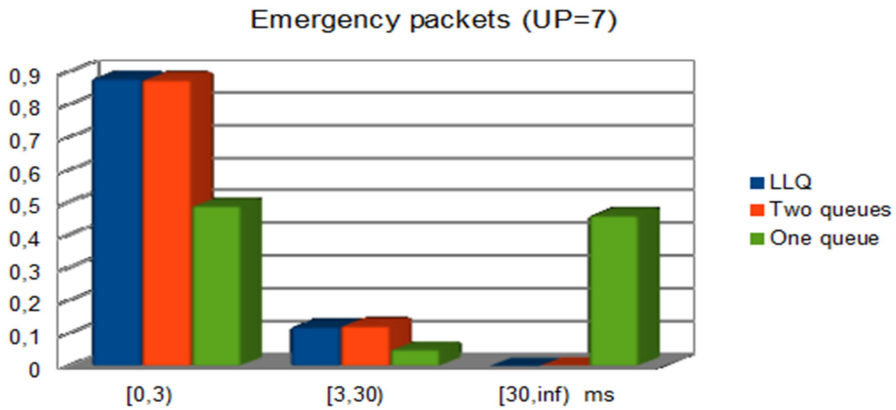

Figure 26:The latency of emergency packets received by the BNC

c. Energy consumption:

The consumed energy histogram presented in Figure 27 shows the average consumed energy per all sensor nodes in the WBAN for each of the three queueing strategies.

We notice from this figure two remarks. First, the consumed energy in the IEEE 802.15.6 standard while using one queue is higher than while using LLQ strategy. The second point to notice is that the amount of the consumed energy rises while increasing the percentage of emergency packets. This observation is mainly due to the queueing strategy and the type of radio receiver used by the standard. As known the time spent in transmitting reduces the reception/listening time which consume more energy as shown in Table 9. So increasing the percentage of emergency packets that can be sent in both

EAP and RAP phases will increase the number of transmitted packets. While we use only one queue the phenomena of the head of line blocking occurs in the EAP phase and will block the sent of packets.

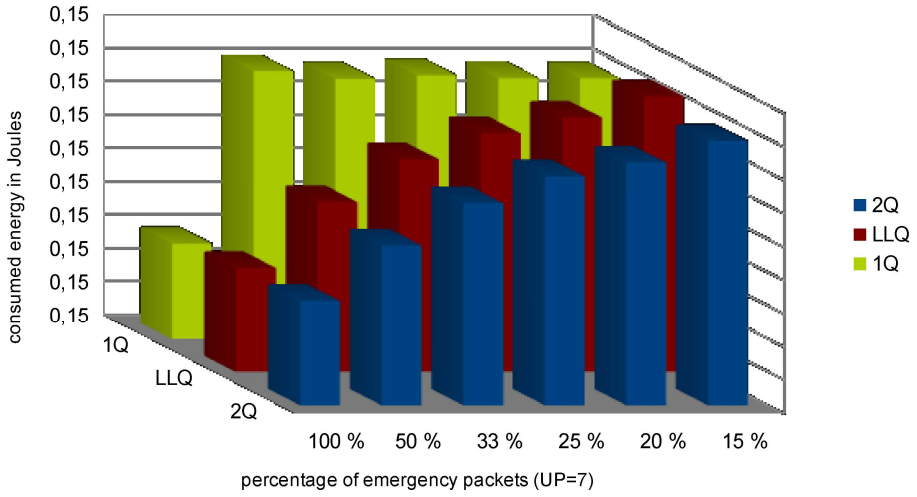

Figure 27: Consumed energy per queueingstrategies in joules

5.4 **Conclusion**

In this chapter, we have evaluated the performances of the IEEE 802.15.6 standard in terms of energy consumption, latency, packets delivery rate, and packets breakdown at the MAC layer while using different queuing strategies. We demonstrated that the queuing mechanism over the IEEE 802.15.6 has a big influence on the network's performances. We have shown the effectiveness of the LLQ queuing strategy in performing the performance of the IEEE 802.15.6, unlike the one queue strategy which degrades the hall network performances.

6 A RENEWAL THEORY-BASED ANALYTICAL MODEL FOR THE CONTENTION ACCESS OF IEEE 802.15.6 CSMA/CA

To provide a general analytical model allowing the study of the IEEE 802.15.6 CSMA/CA access scheme, in terms of latency and packets breakdown at the MAC layer, we propose two complementary sub-models as shown in Figure 28. Firstly, we investigate an analytical sub-model depicting the Backoff process of the IEEE 802.15.6 based CSMA/CA while assuming that sensor nodes can generate heterogeneous traffic in terms of priority. In the saturation regime, where each node has at least one packet waiting for transmission and with the assumption that the sensor nodes generate heterogeneous traffic, it's becoming necessary to define the scheduling strategy at the MAC layer. We have adopted the M/G/1 with non-preemptive priority to meet the QoS differentiation (traffic prioritization) provided by the IEEE 802.15.6 standard. Among the calculated metrics from the first model; the mean delay experienced by nodes to execute the CSMA/CA Backoff process, which is carried out from the instant when the packet leaves the queue until its successful transmission or its dropping. This delay will serve as the service time of our queueing model.

In Figure 29, we illustrate the difference between how heterogeneous traffic is handled in previous models and our analytical model. In Figure 29.a, the WBAN is formed by many sensor nodes; each of them generates only one type of traffic (temperature or Blood pressure…). However, in Figure 29.b, each node can generate many types of traffic with different user priorities (periodic temperature, critical temperature events report …). In both scenarios, our proposed analytical model can be used to evaluate WBAN performances. However, previous proposed models can only be used in the scenario shown in Figure 29.a.

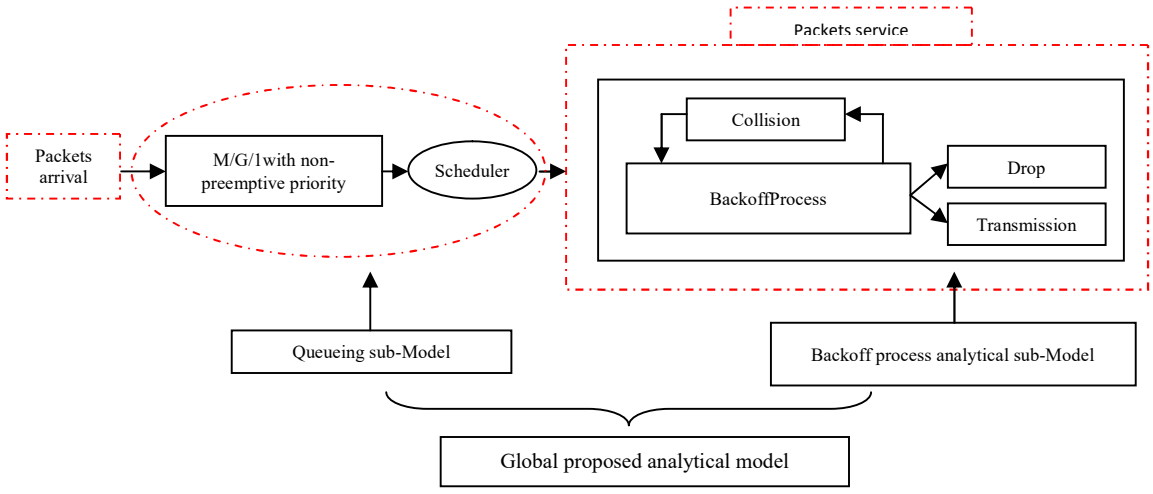

Figure 28: The architecture of the proposed analytical model

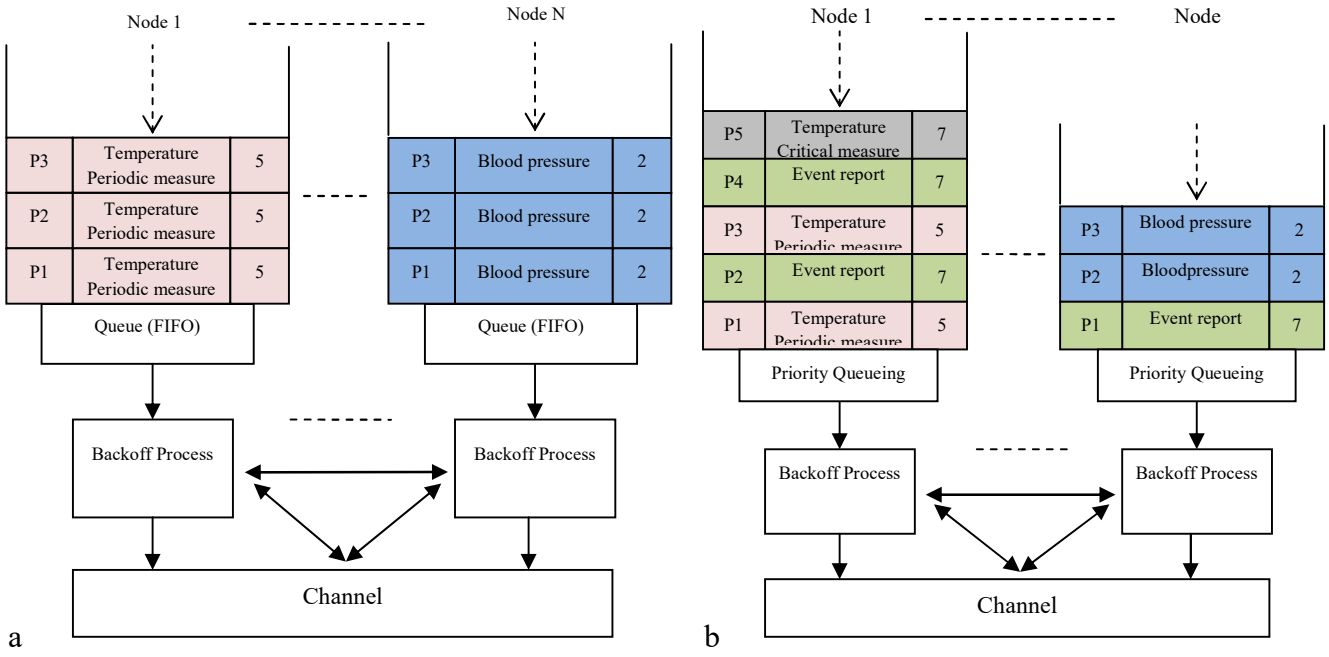

Figure 29: Heterogeneous traffic at: (a) WBANs level, (b) sensor nodes level

To carry out the proposed model, we consider a WBAN with a one-hop star topology, consisting of a BNC and up to $mMaxBANSize$ heterogeneous sensor nodes. All sensor nodes including the BNC are assumed within the transmission range of each other, so there is no hidden node problem. The network operates with the IEEE 802.15.6 in a beacon mode with superframes in which all sensor nodes are synchronized. Only the EAP and RAP phases are considered with CSMA/CA access scheme and immediate Ack policy. We assume that there are neither sensing nor transmission errors, so that transmitted packets are lost only due to the collisions occurred by simultaneous transmissions. We assume also that all sensor nodes transmit packets with the same length and that all sensor nodes generate heterogeneous traffic in terms of user priority and store it in a local queue if it cannot be immediately transmitted. We finally assume that sensor nodes operate in a saturated traffic regime in which it is supposed that the nodes have at least one packet in their queue at any time.

6.2 Renewal-reward theorem-based contention process analytical model:

From the description of the IEEE 802.15.6 CSMA/CA access scheme in chapter3, we notice that the evolution of the Backoff process activities at the MAC layer over a large period can be viewed as a renewal reward process [65]. As depicted in Figure 30, WBANs' nodes reset their Backoff parameters to the default values for each new packet. During each Backoff stage, the tagged node i decrements its

BC only if the channel is sensed idle and it remains enough time in the RAP phase to complete the packet transmission. At the end of each Backoff stage $BS_{i,k}^{j}$, the node performs a transmission attempt, if a collision occurs, the node regenerates its BC and starts the next Backoff stage. The node repeats this process until the successful transmission of the packet or its dropping due to exceed the retry limit$R$. Thus, we consider in our model that the renewal cycle starts from the first stage of the Backoff process until the successful transmission of the packet or its dropping, where the end of each Backoff stage is considered as the earned reward associated with the renewal cycle.

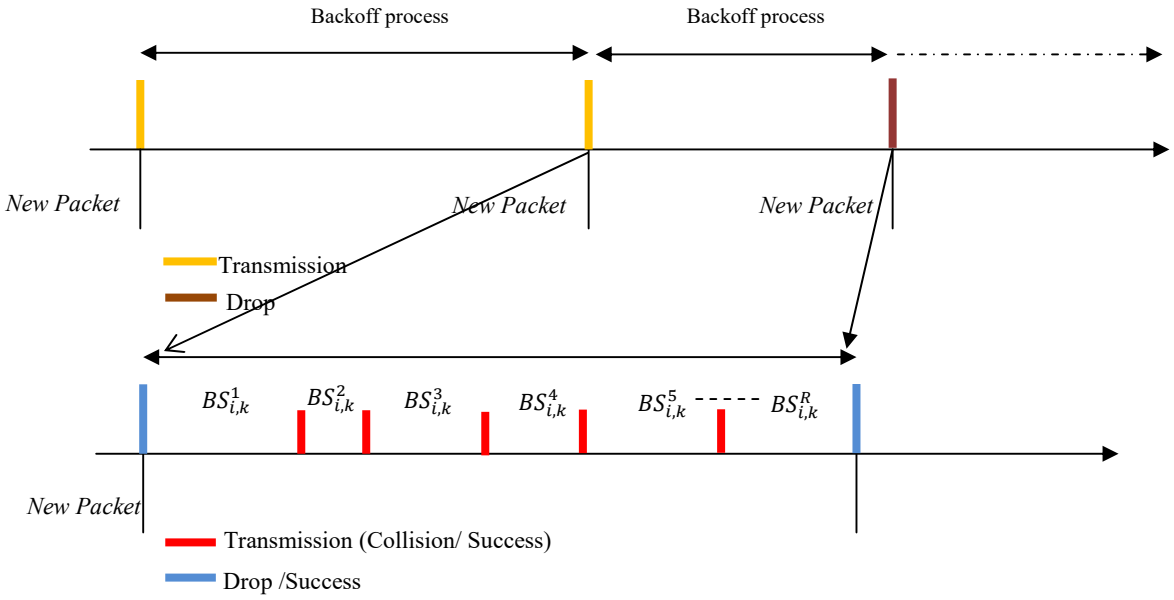

Figure 30: IEEE 802.15.6 Backoff process as a Renewal reward process

To carry out our model, we define $\tau_{i,k}$as the probability of access to the channel (transmission) by a tagged node i executing a priority-class-k packet Backoff process. This probability depends on the number of nodes contending the access to the channel and the priorities of their packets. From the renewal reward theorem, we can derive the access probabilities as follows:

$$\tau_{i,k} = \frac{E(N\_Attempt_{i,k})}{E(BC_{i,k})} \qquad (6)$$

Where $E(N\_Attempt_{i,k})$ represents the mean number of performed attempts by a tagged node $i$to send a priority-class-k packet and$E(BC_{i,k})$ depicts the mean Backoff duration in slots experienced by this node until the successful transmission or the drop of the packet. We calculate at each node i the access probabilities for all packets' priority classes. Thus, our model allows calculating performance metrics for each node separately as well as for the overall WBAN, the aspect that was not handled in

previous works, in which they provided performances for each priority class regardless of the type of the node and its physical characteristics.

To derive the values of $E(N\_Attempt_{i,k})$ and $E(BC_{i,k})$, we define $q_{i,k}$ as the probability that the medium is sensed idle by a tagged node i during the Backoff countdown of a priority-class-k packet and remains idle until the transmission of the packet (no simultaneous transmissions) and $P_{k,Idle}$ as the probability that the channel is sensed idle during a CSMA slot of the Backoff process of a priority-class-k packet.

The probability $q_{i,k}$ that other nodes do not access the channel during the CSMA slot in which the BC reaches zero is given by the following expression:

$$q_{i,k} = \begin{cases} \prod_{\substack{n=1 \\ n\neq i}}^{N} \prod_{p=0}^{7} (1-\tau_{n,p}) & if\ k = 0\ to\ 6 \\ \prod_{\substack{n=1 \\ n\neq i}}^{N} \prod_{p=0}^{7} (1-\tau_{n,p}) \frac{Rap}{Eap+Rap} + \prod_{\substack{n=1 \\ n\neq i}}^{N} (1-\tau_{n,7}) \frac{Eap}{Eap+R} & if\ k = 7 \end{cases} \quad (7)$$

Where, *Rap* and *Eap* are the lengths in slots of the RAP phase and the EAP phase, respectively.

In WBANs operating with the IEEE 802.15.6 MAC protocol, nodes can transmit all types of packets during the RAP phase and send only emergency ones during the EAP phase. Toward this aim, the probability $q_{i,k}$ is bound to the priority-class k of the packet as mentioned in the above equation.

To calculate $P_{k,Idle}$, we consider the channel state for two consecutive CSMA slots. By the Law of Total Probability in classical probability theory [66] and by assuming that the idle probability is constant over the Backoff process, we derive the probability that the channel is idle in the next CSMA slot according to the probability of being idle $P_{k,Idle}$ or busy $1 - P_{k,Idle}$ in the current CSMA slot as follows:

$$P_{k,Idle} = P_{k,(Idle/Idle)} P_{k,Idle} + P_{k,(Idle/busy)} (1 - P_{k,Idle}) \quad (8)$$

$P_{k,(Idle/busy)}$ is the conditional probability that the channel is busy in the current CSMA slot and becomes idle in the next one and $P_{k,(Idle/Idle)}$ is the conditional probability that the channel is idle in the current CSMA slot and remains idle in the next CSMA slot.

$P_{k,(Idle/busy)}$ may also represent the probability that the node which already gained the contended allocation finishes the transmission of at most Nbr packets at the previous CSMA slot. Hence, the probability $P_{k,(Idle/busy)}$ can be expressed as follows:

$$P_{k,(Idle/busy)} = \begin{cases} \frac{1}{Nbr \times T_{Trans}} & if\ k = 0\ to\ 6 \\ \frac{1}{Nbr \times T_{Trans}} \times \frac{Rap}{Eap+Rap} + \frac{1}{Nbr_7 \times T_{Trans}} \times \frac{Eap}{Eap+Rap} & if\ k = 7 \end{cases} \quad (9)$$

Where Nbr_7 and Nbr represent the mean number of packets that can be sent by nodes having gained the contended allocation with the priority-class-7 and priority-class-k packets ($k = 0..7$), respectively. And T_{Trans} represents the mean transmission time of packets.

The channel will remain idle in the next CSMA slot only if none of WBAN's nodes access the channel during this current CSMA slot, as a result, $P_{k,(Idle/Idle)}$ is given as follows:

$$P_{k,(Idle/Idle)} = \begin{cases} \prod_{n=1}^{N} \prod_{p=0}^{7} (1 - \tau_{n,p}) & if\ k = 0\ to\ 6 \\ \prod_{n=1}^{N} \prod_{p=0}^{7} (1 - \tau_{n,p}) \frac{Rap}{Eap+Rap} + \prod_{n=1}^{N} (1 - \tau_{n,7}) \frac{Eap}{Eap+Rap} & if\ k = 7 \end{cases} \quad (10)$$

Using the probability defined in equation (07), we can derive $E(N\_Attempt_{i,k})$ and $E(BC_{i,k})$ as follows:

$$E(N\_Attempt_{i,k}) = \left(\sum_{l=0}^{R} (1 - q_{i,k})^{l} \times q_{i,k} \times (l+1)\right) + \left((1 - q_{i,k})^{R+1} \times (R+1)\right) \quad (11)$$

$$E(BC_{i,k}) = \left(\left(\sum_{l=0}^{R} (1 - q_{i,k})^{l} \times q_{i,k} \times \sum_{s=0}^{l} AvgCW_{k,s}\right) + \left((1 - q_{i,k})^{R+1} \times \sum_{s=0}^{R} AvgCW_{k,s}\right)\right) \times E(decrement_{i,k,Nbr_k}) \quad (12)$$

$$AvgCW_{k,s} = \frac{W_{k,s}+1}{2} \quad (13)$$

Where the entity $AvgCW_{k,s}$ represents the average value of the BC of priority-class-k packets at the s^{th} Backoff stage and $(1 - q_{i,k})^{l} q_{i,k}$ depicts the probability that the packet is successfully transmitted after the l^{th} attempt. The first terms in (11) and (12) represent the case where the packet is successfully transmitted after l^{th} attempt, while the second terms indicate that the packet is dropped after exceeding the retry limit R. $E(decrement_{i,k,Nbr_k})$ represents the mean delay in slots between two successive decrements of the BC of a priority-class-k packet in a node i. As we explained previously, nodes

decrement their BC only if the channel is sensed idle and there is enough time to complete the transmission in the current Rap phase. So, $E(decrement_{i,k,Nbr_k})$ will depend on the mean number of occupied slots by other nodes and the mean number of CSMA slots while the BC is locked due to the insufficient time remaining in the RAP phase to complete the transmission. We consider that the average channel occupation time by WBAN's nodes can be presented by the mean required time to complete the transmission of at least one packet by the node that obtains the contended allocation. According to the IEEE 802.15.6 standard, nodes can send at most four packets during an obtained contended allocation with an emergency packet and can send only one or two packets if they obtain it with low priority packet. Thus, $E(decrement_{i,k,Nbr_k})$ can be expressed for each node i by the following equation:

$$E(decrement_{k,Nbr_k}) = \begin{cases} \sum_{j=0}^{Nbr_k}(1-P_{k,Idle})^{j\times T_{Trans}} P_{k,Idle}(1+j\times T_{Trans}) & if\ k=7 \\ p_{k,Nbr_k}\times Eap + \sum_{j=0}^{Nbr_k}(1-P_{k,Idle})^{j\times T_{Trans}} P_{k,Idle}(1+j\times T_{Trans}) & if\ k=0..6 \end{cases} \quad (14)$$

Where, p_{k,Nbr_k} represents the probability, that the remaining time in the Rap phase is not enough to complete the transmission of Nbr_k non-emergency packets, during an obtained contended allocation.

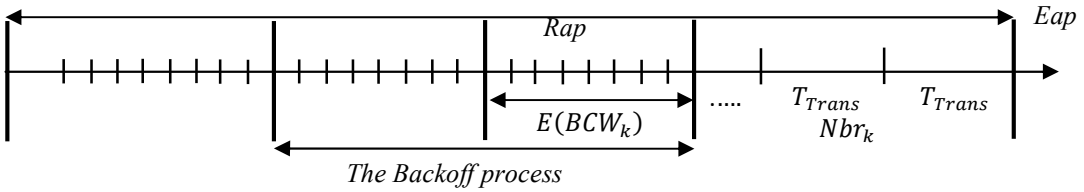

Figure 31: Non-emergency packets Backoff process during the RAP phase

As described in Figure 31 the probability p_{k,Nbr_k} can be expressed as follows:

$$p_{k,Nbr_k} = \frac{1}{(Rap - E(BCW_k) - Nbr_k \times T_{Trans})} \quad (15)$$

$E(BCW_k)$ depicts the mean required time to finish the Backoff stage, which depends on the mean contention window length $W_{k,s}$ as illustrated in the following equation:

$$1 < E(BCW_k) < \frac{\sum_{S=0}^{R} AvgCW_{k,S}}{R} \quad (16)$$

By supposing that the probability that a node detects that it has not enough time to complete the Backoff process is uniformly distributed over the previous interval, we can derive $E(BCW_k)$ as follows:

$$E(BCW_k) = \frac{1+\frac{\sum_{S=0}^{R} AvgCW_{k,S}}{R}}{2} \qquad (17)$$

6.3 Mean contention delay of the IEEE 802.15.6 CSMA/CA Backoff process:

We define the mean contention delay of priority-class-k packets $E(CD_{i,k})$ as the average duration elapsed from the instant a packet becomes the head-of-line at the MAC queue until its successful transmission or its dropping, it can be expressed as follows:

$$E(CD_{i,k}) = p\_Succ_{i,k} \times E(CD\_Succ_{i,k}) + p\_Drop_{i,k} \times E(CD\_Drop_{i,k}) \qquad (18)$$

$$p\_Drop_{i,k} = (1 - q_{i,k})^{R+1} \qquad (19)$$

$$p\_Succ_{i,k} = 1 - p\_Drop_{i,k} \qquad (20)$$

Where,

- $p\_Succ_{i,k}$ is the probability that a priority-class-$k$packet is successfully delivered
- $p\_Drop_{i,k}$ is the probability that it is dropped after exceeding the retry limit R.
- $E(CD\_Succ_{i,k})$ is the mean contention delay in slots of successfully transmitted priority-class-k packets
- $E(CD\_Drop_{i,k})$ is the mean contention delay in slots of the dropped priority-class-k packets.

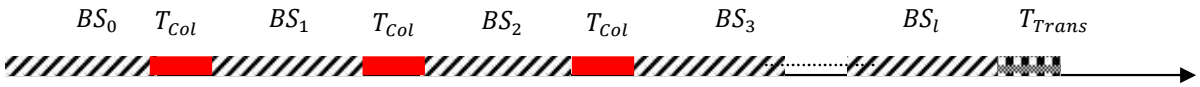

Figure32: Backoff process evolution for successfully transmitted packets

As shown in Figure32, the mean contention delay of successfully transmitted priority-class-k packets $E(CD\_Succ_{i,k})$ is the sum of:

1. The mean Backoff duration in slots experienced by a tagged node before the successful transmission $E(B\_Succ_{i,k})$, which represents the sum of all Backoff stages BS_l;

2. The average time in slots wasted in possible collisions before the successful transmission $E(Col\_Succ_{i,k})$;

3. The transmission time T_{trans}, calculated in μs, then converted on number of slots.

$$E(CD\_Succ_{i,k}) = E(Col\_Succ_{i,k}) + E(B\_Succ_{i,k}) + T_{Trans} \quad (21)$$

Where,

$$E(B\_Succ_{i,k}) = \left(\sum_{l=0}^{R}(1-q_{i,k})^{l} \times q_{i,k} \times \sum_{s=0}^{l} AvgCW_{k,s}\right) \times E(decrement_{i,k}) \quad (22)$$

$$E(Col\_Succ_{i,k}) = \left(\sum_{l=0}^{R}(1-q_{i,k})^{l} \times q_{i,k} \times (l+1)\right) \times T_{Col} \quad (23)$$

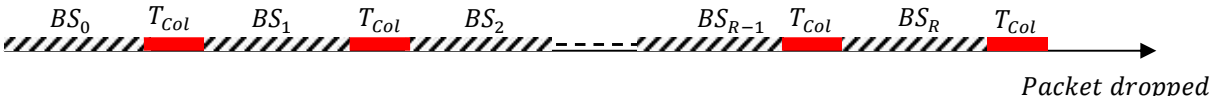

Figure 33: Backoff process evolution for dropped packets

On the other hand, as shown in Figure 33, the mean contention delay experienced by dropped priority-class-k packets $E(CD\_Drop_{i,k})$ is the sum of:

- The mean Backoff duration experienced by packets before their dropping after exceeding the retry limit $RE(B\_Drop_{i,k})$.
- The average time wasted in possible collisions before packets dropping $E(Col\_Drop_{i,k})$.

$$E(CD\_Drop_{i,k}) = E(B\_Drop_{i,k}) + E(Col\_Drop_{i,k}) \quad (24)$$

Where,

$$E(B\_Drop_{i,k}) = \left(\sum_{s=0}^{R} AvgCW_{k,s}\right) \times E(decrement_{i,k}) \quad (25)$$

$$E(Col\_Drop_{i,k}) = (R+1) \times T_{Col} \quad (26)$$

The transmission time T_{Trans} and the collision time T_{Col} are given by the following equations [5], [67]:

$$T_{Trans} = T_{data} + T_{pSIFS} + T_{I-Ac} \quad (27)$$

$$T_{Col} = T_{data} + T_{pSIFS} + T_{timeout} \quad (28)$$

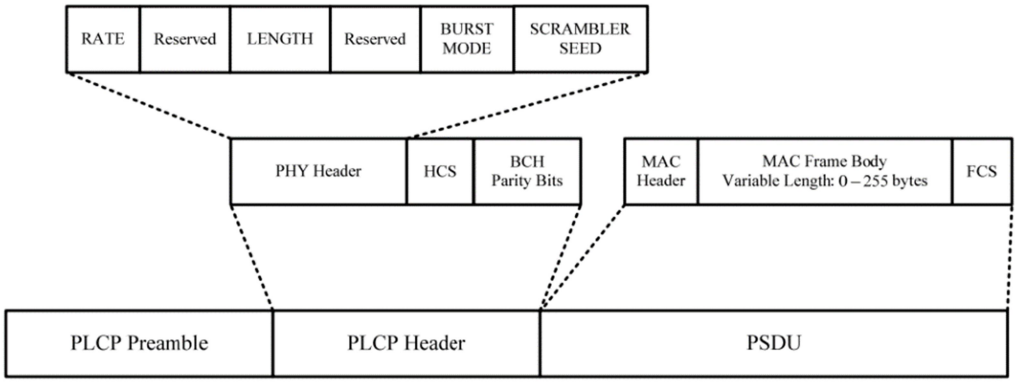

Figure34: IEEE 802.15.6 PPDU structure for NB Physical Layer [5]

As shown in Figure34, the transmission duration of a packet (PPDU) in the narrow band is defined as the transmission of the concatenation of the PLCP preamble, the PLCP header, and the PSDU. According to the IEEE 802.15.6 standard the value of this duration is given as follows:

$$T_{data} = T_s \left(N_{preamble} + N_{header} \times S_{header} + \frac{N_{PSDU}}{log_2(M)} \times S_{PSDU} \right) \quad (29)$$

$$N_{PSDU} = (N_{MACheader} + N_{MACFrameBody} + N_{FCS}) \times 8 \quad (30)$$

Where, the physical parameters: $T_s, N_{preamble}, N_{head}$, S_{header}, $S_{PSDU}, N_{PSDU}, N_{MACheader}$, $N_{MACFrameBody}$ and N_{FCS} are given in the IEEE 802.15.6 standard according to the frequency band used for the communication between the BNC and nodes.

6.4 M/G/1 with non-preemptive priority queueing model:

Without adequate queueing and scheduling strategies to promote the transmission of high emergency packets, WBANs operating the IEEE 802.15.6 standard may not be able to ensure an efficient QoS for high emergency packets. Priority queues form an important class of queueing strategies where arrival packets are distinguished according to their priorities and divided into Kpriority classes. The scheduler serves packets with high priority before those with lower priority [68]. In our model, we assume that emergency packets have an absolute priority over non-emergency packets but are not allowed to interrupt their transmissions. This priority rule is therefore called non-preemptive [69]. The analytical

study of the proposed queueing model allows measuring many performance metrics such as the mean waiting time and the mean number of packets in the queue and the whole system.

We consider in our queueing model an M/G/1 priority queue with K classes of packets [70], where arrivals are Markovian (Poisson process), service times have a General distribution and there is a single server (wireless medium). We denoted by: λ_{pr} the priority-class-pr arrival rates, $E(X_{pr})$ the mean service time (Backoff process) and $\lambda_{pr} \times E(X_{pr})$ the utilization of the service by priority-class-pr packets.

We define the traffic load of a priority-class-pr as:

$$\rho_{pr} = \sum_{j=pr}^{7} \rho_j \qquad (31)$$

$$\text{Where, } \rho_j = \lambda_j E(X_j) \qquad (32)$$

In this part, we do not consider the packets' dropping due to the buffer overflow. Thus, for the stability of the proposed queueing system, the total traffic load must satisfy the following condition:

$$\sum_{pr=0}^{K-1} \rho_{pr} \leq 1 \qquad (33)$$

According to the mean value approach [71], we can compute for a queueing model the mean number of packets and the mean sojourn time, without knowing stationary probabilities. This approach is based on Little's formula [72] and the Poisson Arrivals See Time Averages (PASTA) property [73]. By assuming that the queue service discipline is non-preemptive and that within each priority class the discipline is: First In, First Out, the arrival of a new packet finds $E(L_{pr}^{q})$ packets of each class-pr, waiting in the queue and a priority-class-pr packet in the service with a probability ρ_{pr}. The waiting time in the queue $E(W_k)$ of a new arrived packet depends on its priority k and can be expressed as follows:

- For the higher priority class ($pr = 7$), the newly arrived packet has to wait for packets of its class that arrived before and for the required time to finish the transmission of the packet in service. Thus, the mean waiting time is given as follows:

$$E(W_7) = E(R) + E(L_7^q)E(X_7) \qquad (34)$$

By Little's law we have:

$$E\left(L_{pr}^{q}\right) = \lambda_{pr} E\left(W_{pr}\right) \qquad (35)$$

Combining equations (34) and (35) we obtain:

$$E(W_7) = E(R) + E(W_7)\rho_7 \qquad (36)$$

$$E(W_7) = \frac{E(R)}{(1-\rho_7)} \qquad (37)$$

- For the lower priority classes (pr = 0 ... 6), a newly arrived packet has to wait for packets of its class that arrived before and all for all packets with higher priority already in the queue. The packet has to wait also to all higher priority packets arrived while it waits for the service. The mean waiting time in the queue can be expressed as follows:

$$E\left(W_{pr}\right) = E(R) + \sum_{j=pr}^{7} E\left(L_j^q\right) E\left(X_j\right) + E\left(W_{pr}\right) \qquad (38)$$

Substituting $E\left(L_{pr}^{q}\right)$ from equation (35) into the second term in equation (37), we obtain:

$$E\left(W_{pr}\right) - E\left(W_{pr}\right) \sum_{j=pr+}^{7} \lambda_j E\left(X_j\right) = E(R) + \sum_{j=pr}^{7} \lambda_j E\left(W_j\right) E\left(X_j\right) \qquad (39)$$

Using the traffic load defined in (38) we obtain:

$$E\left(W_{pr}\right)(1 - \rho_k - \rho_{pr+1}) = E(R) + \sum_{j=pr+1}^{7} \rho_j E\left(W_j\right) \qquad (40)$$

$$E\left(W_{pr}\right) = \frac{E(R) + \sum_{j=pr+}^{7} \rho_j E\left(W_j\right)}{(1-\rho_{pr}-\rho_{k+1})} \qquad (41)$$

From equations (37) and (41) we obtain the mean waiting time in the queue of the second priority class packets (pr = 6) as follows:

$$(W_6) = \frac{E(R)}{(1-\rho_7)(1-\rho_6-\rho_7)} \qquad (42)$$

Where, $E(R)$ represents the mean required time to finish the transmission of a packet in service. The value of $E(R)$ is developed in [69] and given as follows:

$$E(R) = \sum_{j=pr}^{7} \frac{\lambda_j E(X_j{}^2)}{2} \qquad (43)$$

Using the Little's law, we derive the mean number of packets in the queue for two packets classes as follows:

$$E(L_7^q) = \lambda_7 \frac{E(R)}{(1-\rho_7)} \qquad (44)$$

$$E(L_6^q) = \lambda_6 \frac{E(R)}{(1-\rho_7)(1-\rho_6-\rho_7)} \qquad (45)$$

By considering a system formed by the queue and the service (Backoff process), we can drive the mean waiting time in the system $E(S_{pr})$ and the mean number of priority-class-pr packets in the system $E(L_{pr})$ as follows:

$$E(S_{pr}) = E(W_{pr}) + E(X_{pr}) \qquad (46)$$

$$E(L_{pr}) = \lambda_{pr} E(S_{pr}) = E(L_{pr}^q) + \rho_{pr} \qquad (47)$$

At a tagged node i, the mean contention delay $E(CD_{i,pr})$ of priority-class-pr traffic, calculated in the first model represents the service time $E(X_{pr})$ of priority-class-pr packets of the proposed queueing model.

6.5 Simulations and results:

As detailed previously, we propose in this thesis an accurate and general analytical model for heterogeneous WBANs. By proposing in the first part, an analytical model for the CSMA/CA Backoff process and in the second part, an adapted priority queue to meet the QoS differentiation offered by the IEEE 802.15.6 standard. By the substitution of equations (11) (12) in equation (6) of the first model, we obtain a non-linear, multivariable system of equations**.** Inspired by previous work such as [11] and [74], we have used the fixed point iterative technique to solve the obtained system. We selected the probability to transmit the packet over the medium $\tau_{i,k}$ as the fixed point and we used Matlab to solve our system. After that, we used the calculated mean Backoff delay from the first model to compute the performance metrics of the proposed queueing model by using Maple. In our simulation, sensor nodes generate all types of packets in terms of priority (eight (8) priorities). The percentage of each user priority is given in each set of simulations. The rest of the simulation parameters are given in Table 11.

Parameter	Value
Frequency Band	2400 MHz to 2483.5MHz
$pSIFS$	75 μs
p (propagation delay)	1 μs
$1/T_s$	600 ksp
S_{header}	4
S_{PSDU}	1
M	4 ($\pi/4 - DQPSK$)
N_{header}	31 bits
$N_{preamble}$	90 bits
$N_{MACheader}$	7 octets
N_{FCS}	2 octets
$N_{MACFrameBody}$	$< pMaxFrameBodyLength$ (255 octets)
T_{I-Ack}	468.4 μs
$mCSMATxLimit$	1
$mMaxBANSize$	< 64 nodes
Buffer size	Infinite (10000 packets)
Simulation time	1000 s (50 iterations)
$N_{MACFrameBody}$	100 Octets $< pMaxFrameBodyLength$
Superframe size	255 Slots

Table 12: IEEE 802.15.6 parameters

We consider in our assessment a simple mapping between the two sub-models by specifying only two classes as shown in Table 12. The first class relates to high emergency traffic, while the second class joins the other classes of traffic together. The first class will have an absolute priority over the second class in which the traffic is served according to its order of arrival. Through this mapping, we try to highlight the impact of the proposed analytical model on handling the emergency traffic for the aim to meet the IEEE 802.15.6 traffic differentiation, in which the emergency traffic is promoted by reserving a dedicated access phase in the superframe and by assigning small contention windows in the CSMA/CA access scheme.

User priority (k) Backoff process model	Priority class (pr) Queueing model
7	7
0,1,2,3,4,5,6	6

Table 13: User priorities mapping between the proposed sub-models

To study the IEEE 802.15.6 based WBANs, we consider two performance metrics; the mean latency and the delivery rates of packets:

a- Delivery rate: To measure the reliability of the network and packets breakdown at the MAC layer, we define $p\_Drop_{i,k}$ as the probability of dropping a priority-class-k packet by a tagged node$i$ after exceeding the retry limit R (no reception of the Ack frame after the last Backoff stage) and $p\_success\_transmit_{i,k,s}$ as the probability of successful transmission after the s^{th} Backoff stage as follows:

$$p\_Drop_{i,k} = (1 - q_{i,k})^{R+1} \qquad (48)$$

$$p\_success\_transmit_{i,k,s} = q_{i,k} \times (1 - q_{i,k})^{s-1} \qquad (49)$$

b- Latency: We define the mean latency of priority-class-k packets as the average duration elapsed from the instant when a packet arrives at the MAC queue until its successful transmission or its dropping. It can be expressed according to the packet priority as follows:

$$Latency_{i,k} = \begin{cases} \frac{E(R)}{(1-\lambda_7 E(CD_{i,7}))} + E(CD_{i,7}) & if\ k = 7 \\ \frac{E(R)}{(1-\lambda_7 E(CD_{i,7}))(1-\lambda_k E(CD_{i,\leq 6})-\lambda_7 E(CD_{i,7}))} + E(CD_{i,\leq 6}) & if\ k = 0 \dots 6 \end{cases} \qquad (50)$$

$$\text{With:} \qquad E(CD_{i,\leq 6}) = \frac{\sum_{z=0}^{6} E(CD_{i,z})}{7} \qquad (51)$$

6.5.1 Measurement and result analysis:

In this section, we carry out several performances' analyses of the IEEE 802.15.6 standard while varying one or more parameters in each set of simulations. Many parameters may influence the behavior of the standard; we quote the number of nodes, the percentage of emergency packets among the total packets, the EAP length, the packets arrival rate, and the number of attempts. For each parameter, we calculate analytically and by simulations:

- The mean latency of both emergency and non-emergency traffic.
- The traffic load for each type of packets, which represents in the queueing theory the utilization of the service by each class of traffic; it is the result of the multiplication of the arrival rate by the mean service time.

- The ratios of the successful transmissions after the 1^{st} attempt, 2^{nd} attempt … R^{th} attempt and the ratio of dropped packets due to an unreceived Ack frame after the R^{th} attempt.

We evaluate the most of the aforementioned parameters with several arrival rates, ranging from 10 p/s to 150 p/s (packet/ second), to show the behavior of the standard under different traffic regimes. To avoid the overloading of results' analysis, we show for each parameter only the graphs corresponding to arrival rates which afford the most effect on this parameter. In the end, we present a performance analysis of the overall WBAN as well as the nodes that compose it separately to show if it is necessary to provide an analytical model, which allows analyzing nodes' performance.

- **Impact of traffic Arrival rate:**

As shown in Figure 35, 36, and 37, we evaluated the IEEE 802.15.6 based WBANs performances while varying the packets' arrival rate from 1 p/s to 200 p/s. We set the retry limit to two (2) (the default value of Castalia simulator), the percentage of emergency packets to 15%, the EAP length to zero (0), and the number of nodes to 12 nodes.

We notice from Figure 36 that the mean latency increases with the increase of the arrival rate. This is explained by the longer time spent during nodes' Backoff processes caused mainly by the extensive use of the medium; The more WBAN's nodes generate traffic, the more collisions occur in the medium, which leads packets to experience more Backoff stages before their successful transmission or their drop. Moreover, by queueing theory, buffered packets in queues have to wait longer before being served, due to the longer time spent in service (Backoff process). In Figure 35, we notice that the high traffic intensity, which leads to high use of the medium, affects the number of dropped packets and the number of attempts before successful transmissions of packets. The more we raise the arrival rate, the more failed packets increase and the more transmitted packets after the first Backoff stage decreases in detriment of transmitted ones after the second Backoff stage. Figure 37 shows that after exceeding 125 p/s, the total traffic load exceeds the stability condition of the queueing system as illustrated in equation (33). For this aim, we present only latency and packets breakdown results with arrival rates of less than 125 p/s.

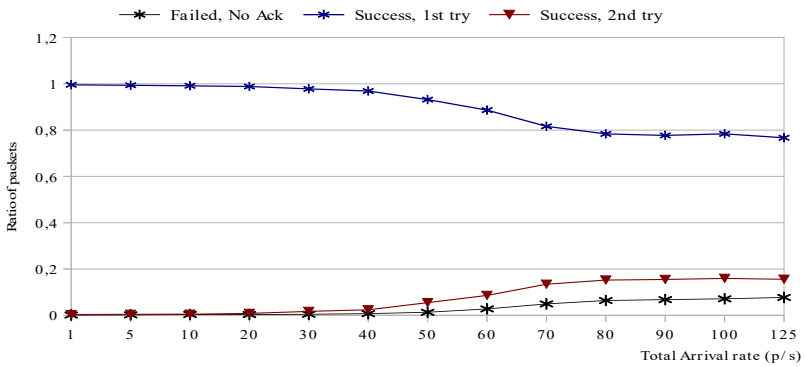

Figure 35: The effect of arrival rate on packets breakdown at Mac Layer

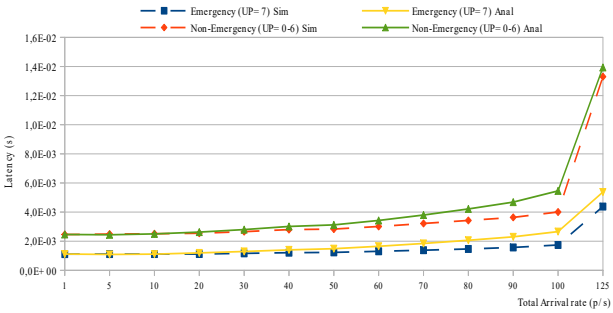

Figure 36: The effect of arrival rate on the average latency

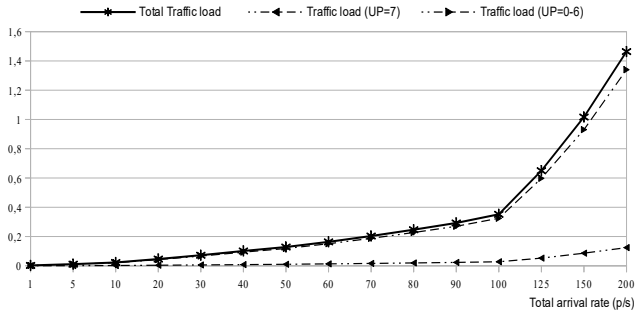

Figure 37: The effect of arrival rate on queueing traffic load

- **Impact of number of nodes:**

To analyze the impact of the number of nodes on WBANs' performances, we vary the number of nodes from 1 to 12 while setting the retry limit to two (2), the percentage of emergency packets to 15%, and the EAP length to zero (0). In this evaluation, we present results with the arrival rates of 50 p/s, 75 p/s, and 100 p/s.

We notice from Figure 38 that in contrast to successful transmissions the amount of failed one's increases while increasing the number of nodes, and it further increases with a high data arrival rate. Besides, the number of attempts before the successful transmission of packets is also influenced by both the arrival rate and the number of nodes.

The more the number of nodes and the arrival rate increases, the more the number of transmitted packets after the second Backoff stage increases at the expense of the transmitted packets after the first Backoff stage. This is mainly due to the rise of contending nodes to access the channel, which results in high channel occupation that leads to high packets' collisions.

From Figures 40, 42, and 44 depicting the traffic load of WBAN's nodes, we notice that the number of nodes and the arrival rate have an important impact on the traffic load of emergency and non-emergency traffic. In contrast to non-emergency traffic load, the emergency traffic load varies slightly. This difference can be explained by the fact that the Backoff process of emergency traffic is smaller than the non-emergency ones due to the gap between related contention windows. Equations (31) and (32) show how the Backoff process can influence the traffic load. Increasing the number of nodes in the network raises the number of collisions due to the high use of the medium, thus resulting in a high amount of experienced time in Backoff processes, which leads to the increase of the latency. Also, as depicted in Figures 39, 41, and 43, we notice that the behavior of the latency differs according to the type of traffic. For the emergency traffic, the increase of latency rate is slightly smaller than for the non-emergency traffic. This is explained by the fact that emergency packets have to wait in the queue only for previously arrived emergency packets. However, non-emergency packets have to wait for all previously arrived packets regardless of their priority. In the figures illustrating the latency, we didn't show the latency when the number of nodes goes over ten (10) nodes in Figure 41 and seven (7) nodes in Figure 43 because the value of the traffic load after these numbers of nodes does not satisfy the queueing system stability condition (total traffic load < 1) as shown in Figures 42 and 44, respectively.

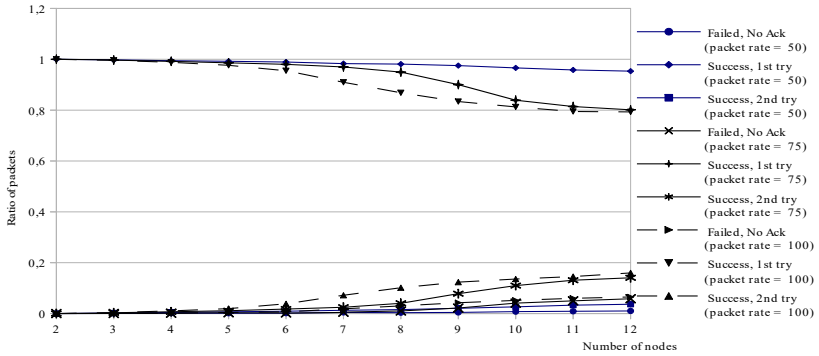

Figure 38: The effect of the number of nodes on packets breakdown at Mac Layer

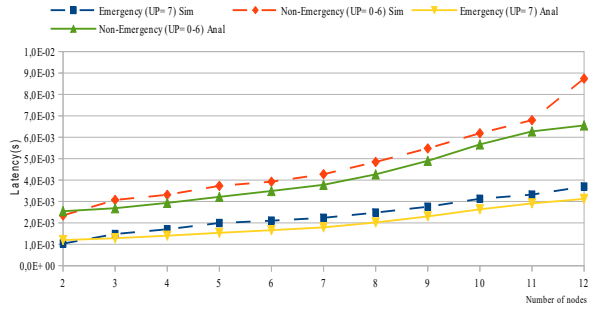

Figure 39: The effect of the number of nodes on the average latency (arrival rate = 50 p/s)

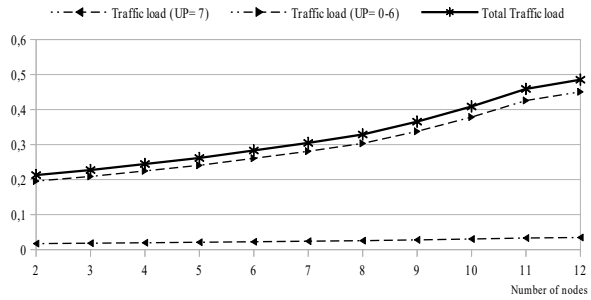

Figure 40: The effect of the number of nodes on queueing traffic load (arrival rate = 50 p/s)

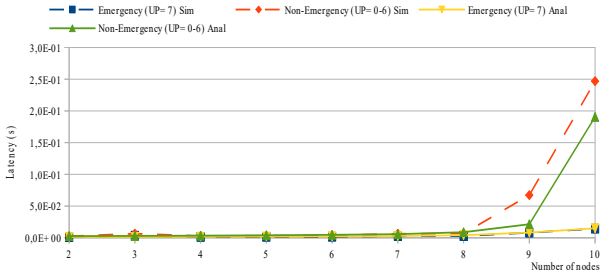

Figure 41: The effect of the number of nodes on the average latency (arrival rate = 75 p/s)

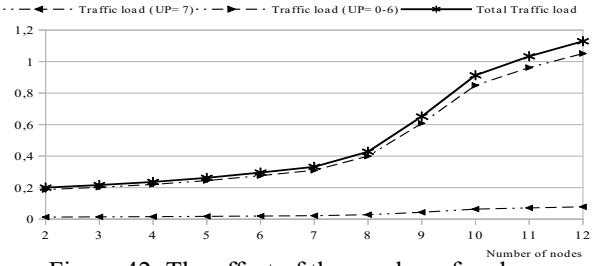

Figure 42: The effect of the number of nodes on queueing traffic load (arrival rate = 75 p/s)

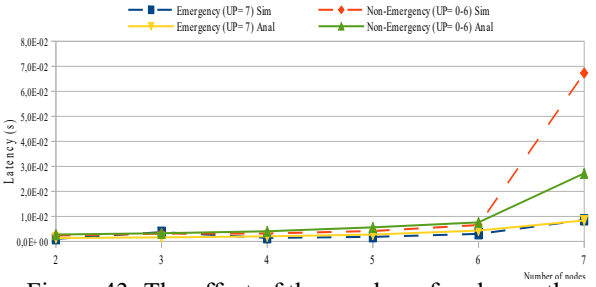

Figure 43: The effect of the number of nodes on the average latency (arrival rate = 100 p/s)

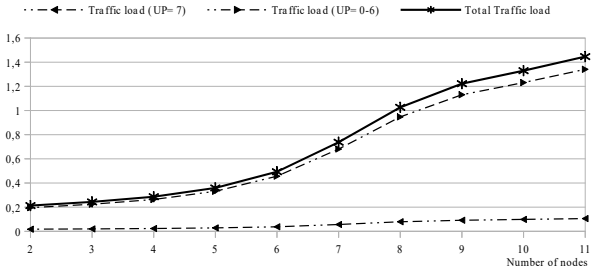

Figure 44: The effect of the number of nodes on queueing traffic load (arrival rate = 100 p/s)

- **Impact of EAP phase's length:**

In this set of simulations, we perform several assessments to study the effect of the EAP phase's length on the standard performances, we set the retry limit to two (2), the percentage of emergency packets to 15%, the number of nodes to five (5) and we present analysis results with the arrival rates 10p/s, 50p/s, and 100p/s.

We notice from Figures 47, 49, and 51 that, as we increase the arrival rate and the EAP length, the non-emergency traffic load increases while the emergency traffic load decreases. As explained in previous analyses, the more we increase the packets arrival rate, the more the communication medium is saturated by WBAN's nodes transmissions, resulting in the increasing of the time spent in the

Backoff process. In addition to that, all non-emergency packets have to wait more in queues by increasing the EAP length, because only emergency packets can be served in this phase. Therefore, the medium saturation and the waiting time in queues justify the variation of the latency in Figures 46, 48, and 50. We notice also, that there are some differences between analytical and simulation recorded latencies. This is explained by the fact that in our analytical model, we do not take into consideration communication errors during beacon frames transmission and during the WBAN setup phase, in which nodes send requests to join the BAN. The same analysis can explain the results of the packets' delivery rate presented in Figure 45. With the increase of the arrival rate, the amount of dropped packets and the transmitted packets after the second Backoff stage decreases to the detriment of the transmitted packets after only the first Backoff stage.

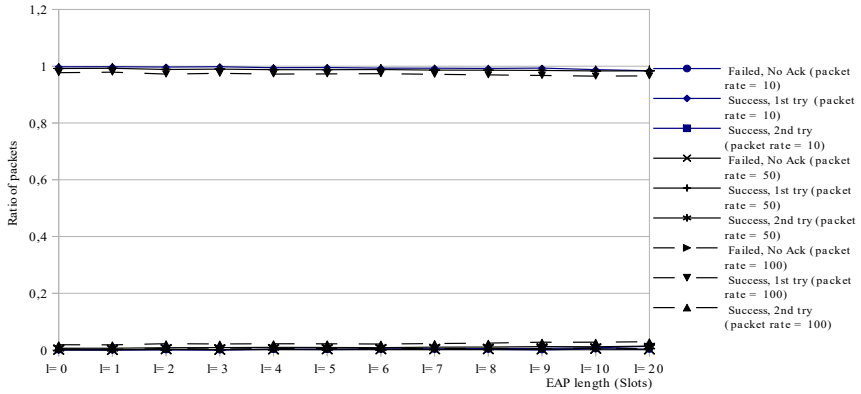

Figure 45: The effect of the EAP length on packets breakdown at Mac Layer

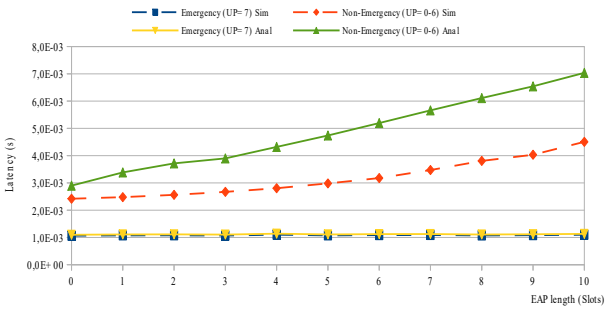

Figure 46: The effect of the EAP length on the average latency (arrival rate = 10 p/s)

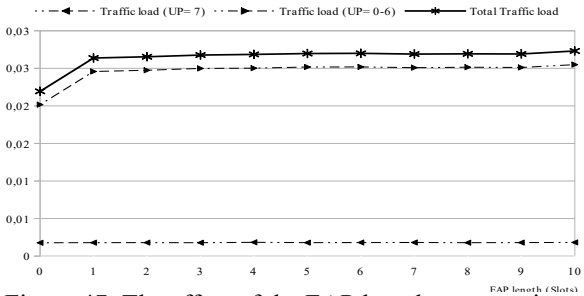

Figure 47: The effect of the EAP length on queueing traffic load (arrival rate = 10 p/s)

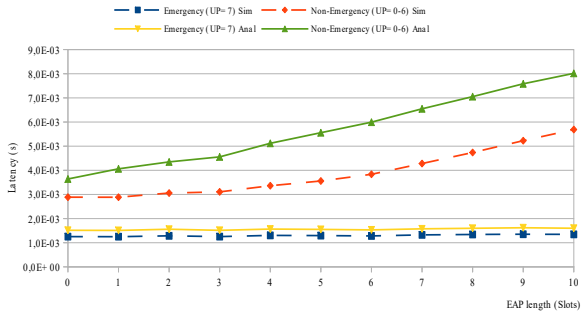

Figure 48: The effect of the EAP length on the average latency (arrival rate = 50 p/s)

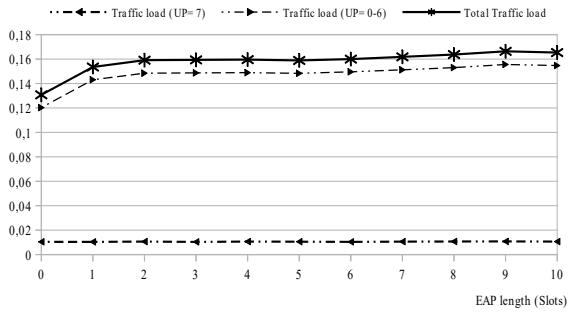

Figure 49: The effect of the EAP length on queueing traffic load (arrival rate = 50 p/s)

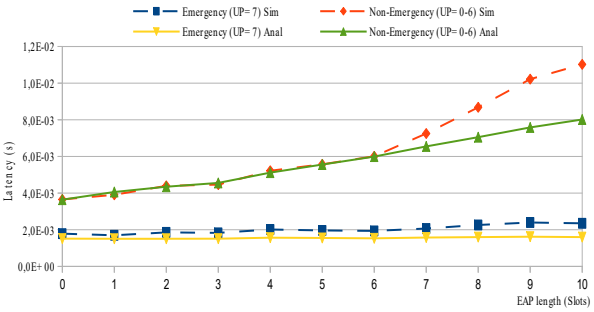

Figure 50: The effect of the EAP length on the average latency (arrival rate = 100 p/s)

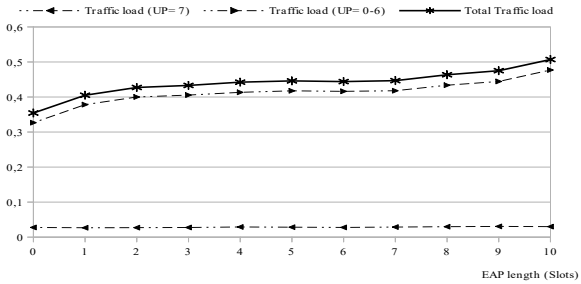

Figure 51: The effect of the EAP length on queueing traffic load (arrival rate = 100 p/s)

- **Impact of Retry limit:**

We analyze in this part, the impact of the retry limit on the mean latency and packets delivery. We set the EAP length to zero (0), the percentage of emergency packets to 15%, and the number of nodes to five (5). We present analysis results for two arrival rates (100 p/s and 150 p/s), For each of them, we provide the packets breakdown at the MAC layer, the latency for emergency and non-emergency traffic as shown in Figures 52, 53, 55, and 56. To consolidate the latency results, we present in Figures 52 and 55 the traffic load for both emergency and non-emergency traffic.

We notice from Figures 52 and 55 depicting the failed and successful transmissions that, as the maximum number of authorized transmission tries raises, the ratio of failed packets decreases, and the ratios of successful transmissions after i^{th} attempt (i= 1..6) increases. To make the recoded results more clear, we do not illustrate in these figures the packets breakdown after the first try, because it has extra higher values compared to other types. In fact, the more the maximum authorized attempts raises, the more the packets have the chance to be successfully transmitted in the following Backoff stage, instead of being dropped in the current one due to collisions. We also notice that the figures 52 and 55 have the same shape, except that the ratio of failed packets is greater with the highest data rate, due to the high

collision rate. We remark the same fact in Figures 53 and 56, in which the latency increases considerably when the packet arrival rate increases. In addition to that, in we only showed Figure 56 the latency results with 0, 1, and 2 as retry limit due to the instability of the queueing system for the values above three (3), with which the total traffic load exceeds one (1) as shown in Figure 57.

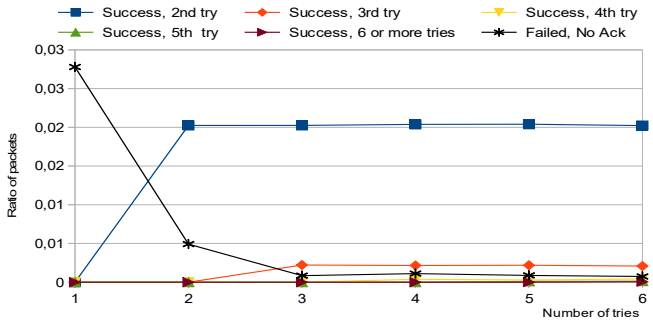

Figure 52: The effect of the max number of tries on packets breakdown at Mac Layer (arrival rate = 100 p/s)

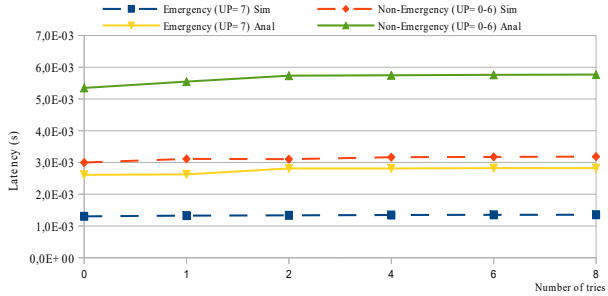

Figure 53: The effect of the max number of tries on the average latency (arrival rate = 100 p/s)

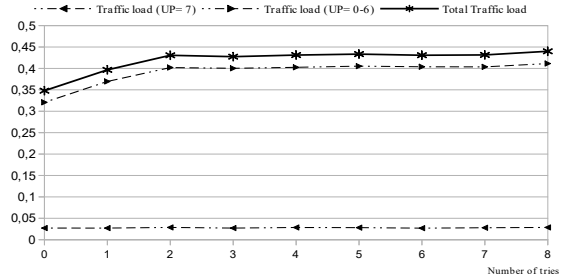

Figure 54: The effect of the max number of tries on queueing traffic load (arrival rate = 100 p/s)

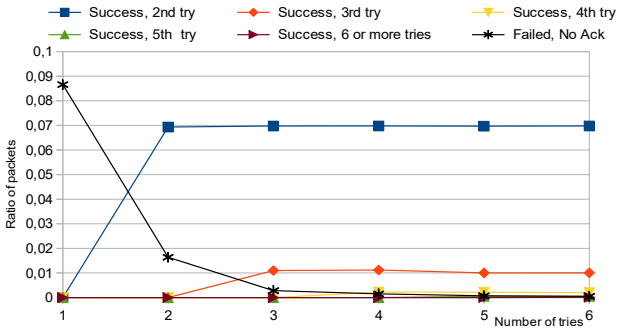

Figure 55: The effect of the max number of tries on packets breakdown at Mac Layer (arrival rate = 150 p/s)

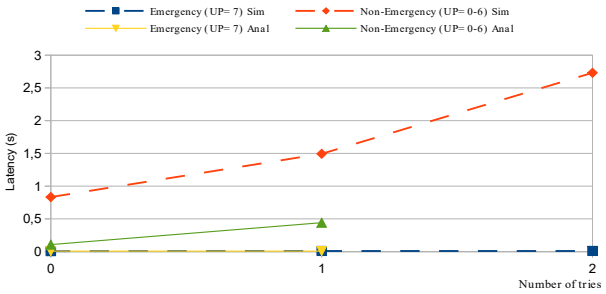

Figure 56: The effect of the max number of tries on the average latency (arrival rate = 150 p/s)

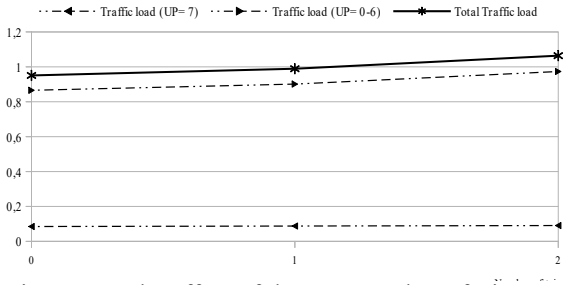

Figure 57: The effect of the max number of tries on queueing traffic load (arrival rate = 150 p/s)

- **Impact of Emergency packet arrival rate:**

We perform in this part, analyses on the impact of varying the amount of emergency packet on the IEEE 802.15.6 based WBANs while setting the EAP length to zero (0), the retry limit to two (2), and the number of nodes to five (5). We notice from Figure 58 that the amount of successfully transmitted packets after the first Backoff stage represents the major part compared to those transmitted after the second Backoff stage and the failed ones after exceeding the retry limit. Moreover, we notice a gap between the recorded results for each arrival rate, which is explained by the extensive use of the medium with high arrival rates.

In Figures 59 and 61, we show the recorded latency for the two arrival rates, while varying the rate of emergency packets. We notice that the mean latency increases while decreasing the amount of generated emergency traffic. This is mainly explained by the difference of the Backoff process experienced time by the two types of traffic; as illustrated in the IEEE 802.15.6 CSMA/CA access scheme description, the more the packet's priority decreases, the more the contention window increases, and vice versa. Besides, the adopted queueing strategy allows for high emergency packets to be served before those with low priority. As a result, the more we increase the rate of emergency packets, the more the non-emergency packets have to wait longer in the queue. Figures 60 and 62 consolidate the obtained results in the latency graphs. Indeed, the increase in the ratio of emergency packets increases the traffic load of non-emergency traffic to the detriment of the emergency one.

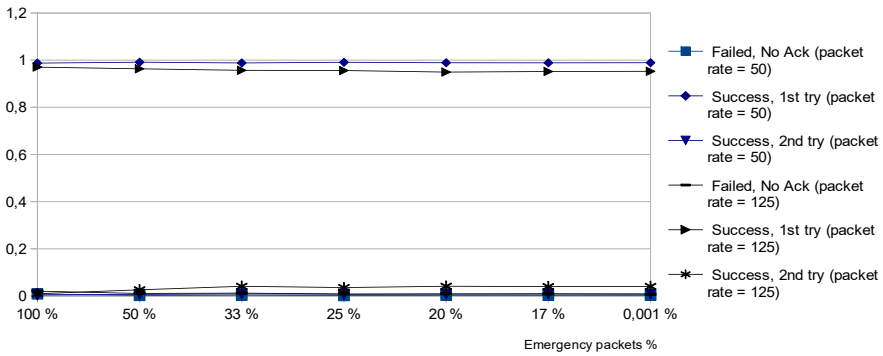

Figure 58: The effect of percentage of emergency packets on packets breakdown at Mac Layer

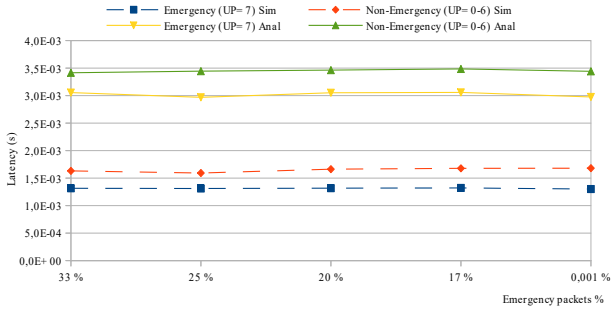

Figure 59: The effect of percentage of emergency packets on the average latency (arrival rate = 50 p/s)

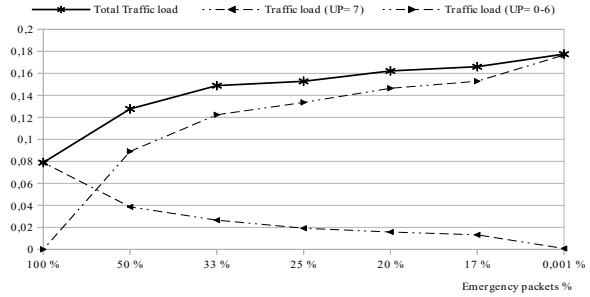

Figure 60: The effect of percentage of emergency packets on queueing traffic load (arrival rate = 50 p/s)

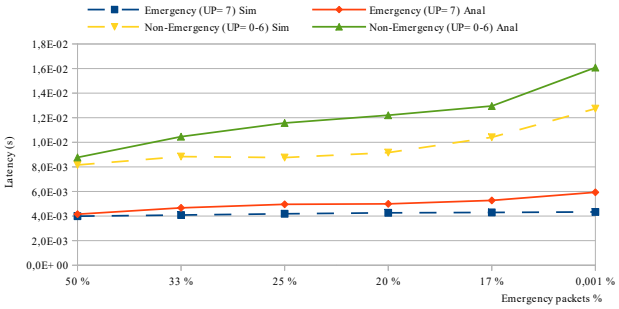

Figure 61: The effect of percentage of emergency packets on the average latency (arrival rate = 125 p/s)

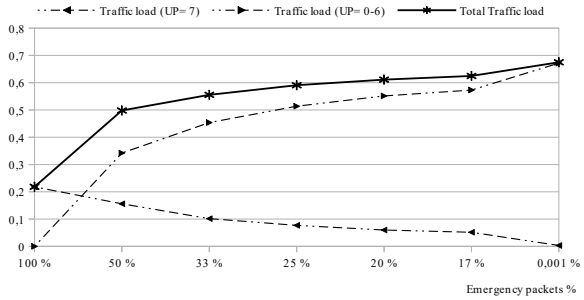

Figure 62: The effect of percentage of emergency packets on queueing traffic load (arrival rate = 125

- **WBAN vs. WBAN's nodes performances:**

As mentioned previously, the proposed analytical model allows performances' study of the overall WBAN's or individual WBANs' nodes. To make the difference clearer between results' analysis for the overall WBAN and individual nodes, we consider in our simulations a WBAN describing a home monitoring of an individual cardiac patient. As described in the ISO/IEEE 11073 Draft standard for Point-of-Care (PoC) medical devices [60], this WBAN incorporates five (5) sensor nodes; to ensure the 3-lead ECG supervision, three (3) electrodes are deployed on the rib cage of the patient. The two other sensors are placed on the left and right arms to measure the SpO2 and blood pressure

respectively. We carry out the analysis of the latency and the number of received packets at the BNC. The description of the considered WBAN is given in Table 4.

Figure 63 shows the recorded mean latency for the overall WBAN and each WBAN's node separately. We observe that the latency differs for each node according to the traffic arrival rate and to the priority. For the non-emergency traffic, we notice that the recorded mean latency for nodes 2 and 3 is equal to zero, and the recorded for nodes 1, 4, and 5 is higher than that recorded for the overall WBAN. This is explained by the fact that nodes 2 and 3 do not generate non-emergency traffic unlike nodes 1, 4, and 5, which generate all types of traffic. Also, we notice that the node 4 has the highest non-emergency latency compared to the other nodes. This is due to that node 4 generates traffic with a higher data rate than nodes 1 and 5, which leads to an increase of the waiting time in the queue for this type of traffic, thereby increasing the global latency.

On the other hand, we notice that the recorded latency for emergency traffic is different from one node to another; the latency in nodes generating only emergency traffic is lower than in nodes generating both, emergency and non-emergency traffic. This is due to the used queueing strategy, in which we adopted a non-preemptive priority. This strategy does not allow emergency packets to interrupt the already started Backoff process by a packet even if it is a non-emergency one. Therefore, it leads to an increase in the whole latency by increasing the waiting time of emergency packets in the queue. As it was the case for non-emergency traffic, we notice that the latency for emergency traffic in node 4 is higher than that of the nodes 1 and 5. This is because nodes 1 and 5 generate emergency traffic with a low rate compared to the node 4, which results an increasing of the waiting time in the queue. The results in Figures 64.a and 64.b illustrate packets breakdown. The first noticeable characteristic is that the mean number of failed packets for the overall WBAN is different from those calculated for each node, separately. As explained for the latency analysis, the traffic arrival rate and its priority have an important impact on the nodes' performances. The traffic with a high arrival rate increases the number of both, received and failed packets, and the opposite is true.

WBAN Nodes		Geometric coordinates	Arrival rate (packet/s)		
			Total traffic	emergency traffic	Non-emergency traffic
0	BNC	x= 0.12, y= 0.30	/	/	/
1	Blood Pressure	x= 1.20, y= 0.30	1	0,17	0,83 (0,11 for each UP)
2	ECG	x= 1.20, y= 0.68	150	150	0
3	ECG	x= 1.50, y= 0.68	125	125	0
4	ECG	x= 1.50, y= 0.38	150	75	75 (10,71 for each UP)
5	Spo2	x= 1,00, y= 0.38	10	3,3	6,7 (0,95 for each UP)
Overall WBAN			87,2	70,694	16,506

Table 14: Home monitoring of an individual cardiac patient WBAN characteristics

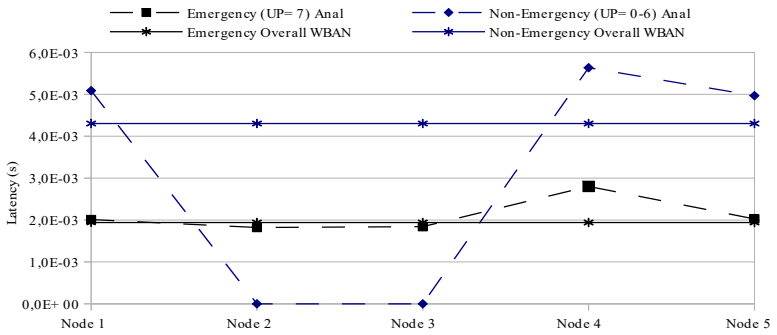

Figure 63: The average latency per node

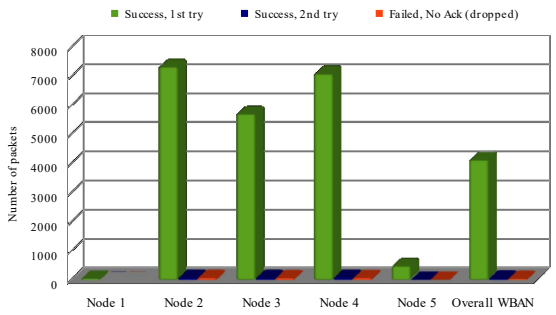

Figure 64.a: Packets breakdown at Mac layer

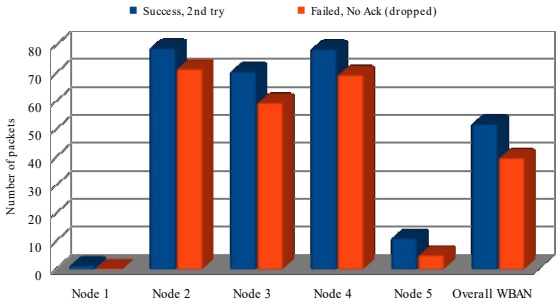

Fig. 62.b: Packets breakdown at Mac layer

From the above results, we conclude that limiting the analyses of WBAN in the mean values of performance metrics may not reflect all WBANs performances, especially in the case where nodes do not have the same configuration and constraints such as the arrival rates and packets' priorities.

6.6 Conclusion

In this chapter, we proposed a general analytical model of the IEEE 802.15.6 based WBANs, with heterogeneous traffic in terms of priority. In the first step, based on the renewal reward process, we provided an analytical sub-model depicting the IEEE 802.15.6 based CSMA/ CA Backoff process. In the second step, an M/G/1 queuing model with non-preemptive priority is proposed to handle emergency traffic at MAC queues. The performance measures obtained by the analytical model were validated by accurate simulations using Castalia Simulator. Results showed that using a queuing model with priority improves the latency and the delivery rate of emergency traffic in detriment of non-emergency ones, which is in a perfect agreement with the IEEE802.15.6 QoS targets. On the other hand, we illustrated how the proposed model can allow the computation of performance measures of individual nodes as well as the overall WBAN, which was not offered by previous analytical models.

7 SERVER-BASED SECURE KEY MANAGEMENT FOR THE IEEE 802.15.6 STANDARD

Since communications in WBANs can carry sensitive information, the IEEE 802.15.6 standard provides for strong security by a security association procedure that identifies a node and the BNC to each other. However, many security vulnerabilities are noticed in the above procedure, especially to the Key Compromise Impersonation (KCI) and the impersonation attacks [59], [57] described in section 2.6.2. In this part, we design a new secure key management and user authentication scheme that aims to improve the IEEE 802.15.6 security, called Server-Based Secure Key Management for the IEEE 802.15.6 standard (SBSKM). The objective of the proposed scheme is to ensure the encryption of all communications starting from the beginning of the security association procedure. Therefore, we extended the security architecture of the standard by including a trusted server, responsible for the creation, initialization, and distribution of encryption keys as well as their renewal, in addition to guaranteeing the identity of the sensors joining the network.

7.1 Principle of the proposed solution against impersonation attack:

The architecture of the proposed solution consists of a set of sensor nodes S_i, a BNC forming a WBAN, each WBAN is unique to a single individual, this same individual will be connected through an external network to a Security Server (SS)as shown in Figure 65, this server is supposed to be powerful equipment. Communication between the BNC and SS is supposed to be secure, as it is provided by technologies and protocols that are not part of the IEEE 802.15.6 standard.

As part of our solution, three types of keys are used:

- K_{msg}: The symmetric key is used for communication between the BNC and the sensors.
- K_{sec}: The unique key for each sensor and only shared with the security server.
- K_{mas}: The key used only to refresh K_{msg}, it is a public key of K_{sec}.

All sensor nodes are initialized with an identity ID_i and a unique and random Security Key (K_{sec}) by the SS, this initialization can only be done via cable, at the server itself, or at the BNC or any other equipment having a secure connection with SS, to keep the K_{sec} out of the band.

Each sensor node wishing to join an open WBAN (accepting new sensor nodes), sends a join message protected by K_{sec} to the SS via the BNC (the BNC will act as a gateway). The SS checks the connection request message and then generates two sub-keys: a Message Key (K_{msg}) and a Master Key (K_{mas}), these latter will be sent back to the BNC if the request is validated. The BNC encrypts K_{msg} with K_{mas} which is the public key of K_{sec}, and sends it to the sensor node.

At the end of the association process, the BNC plans a renewal period for K_{msg} in the number of communication cycles (Superframe).

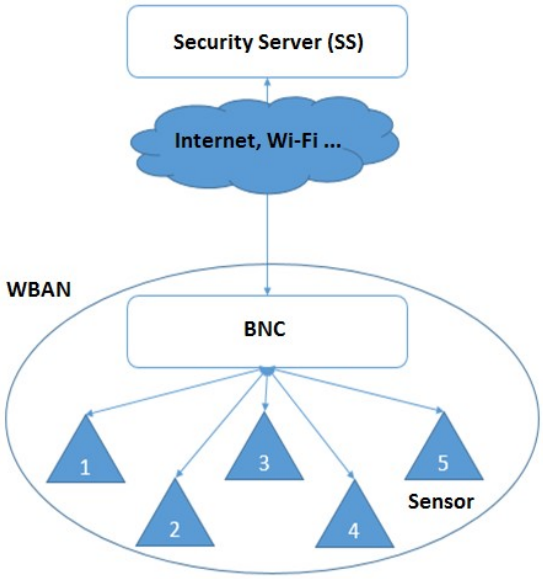

Figure 65: WBAN security architecture proposed by the "SBSKM" protocol

7.2 Solution design and implementation:

- **Sensor initialization:**

The sensor node security initialization is done before it joins a WBAN. During this phase, the secret key based on a unique sensor identifier (*ID*) is generated by the SS and then transmitted to the sensor node via an external network which must be secured to ensure that the key is not disclosed. This can be done either by connecting the sensor directly via cable to the *SS* or to the BNC as a gateway.

$$S_i \leftarrow K_{sec} - SS \qquad (52)$$

Once the keys are stored in the memory of both devices, they are attached to a counter that will be incremented each time the key is used and added to the data transmitted during connection, to protect against replay.

- **Authentication:**

For any message transmitted over the network, encryption and authentication are essential.

The Authentication in our model is ensured by two sub-keys: an encryption key K_e and a signature key K_{mac} using the Authentication Code Message (*MAC*). These two sub-keys are used to encrypt and sign the sensor connection request, resulting in the following message.

$$S_i \rightarrow : \{ d \mid t + \{ d \mid t \} K_{mac} \} K_e \qquad (53)$$

In this message, "d" refers to the data, it includes the sensor *ID* and a key usage counter, "t" the time-stamp. Upon its reception by the *SS*, the message can be decrypted and authenticated, thus guaranteeing the identity of the sensor [18].

Sensors connection

The sensor node sends a connection request in this form:

$$S_i\text{-}CNCT\_REQ \rightarrow BNC \qquad (54)$$

The request protected by K_e and *MAC* as in equation (53), is forwarded by the BNC to the *SS*:

$$BNC - CNCT\_REQ \rightarrow SS \qquad (55)$$

The *SS* checks the encryption, *MAC*, and key usage counter. In case they are valid the *SS* sends to the BNC two keys:K_{mas} and K_{msg} to the corresponding sensor:

$$SS - K_{mas} + K_{msg} \rightarrow BNC \qquad (56)$$

The BNC then transmits to the sensor K_{msg} and a Renewal Counter of RC all encrypted with K_{mas}. RC is the number of superframes after which the K_{msg} is renewed.

$$BNC - \{ K_{msg} + RC \} K_{mas} \rightarrow S_i \qquad (57)$$

Thus, communications are encrypted using K_{msg} for the biometric data collected by the BNC.

- **Key refreshing:**

When the sensor receives K_{msg} from the *SS*, the BNC plans a renewal period of K_{msg} after RC superframes. At the end of each renewal period, all sensor nodes lunch a request of the renewal key from the *SS* via the BNC.

$$S_i\text{-}RNW\_REQ \rightarrow BNC\text{-}RNW\_REQ \rightarrow SS \qquad (58)$$

The SS generates a new Message key $\acute{K}_{msg}$ andattaches it to the sensor's K_{mas} and transmits them to the BNC:

$$SS\text{-}K_{mas} + \acute{K}_{msg} \rightarrow BNC \qquad (59)$$

The BNC encrypts $\acute{K}_{msg}$ attached with RC with K_{mas} and transmits them to the sensor node:

$$BNC\text{-}\{\acute{K}_{msg} + RC\}K_{mas} \rightarrow S_i \qquad (60)$$

It is also important to note that the renewal of K_{sec} planned according to the key resilience and requires going through the initialization process.

The initial connection requires the connection between BNC and the *SS*, it then becomes important, but not essential, because it may be impossible in some cases. To remedy this, the solution plans to continue using the same keys until new ones are obtained.

It should be noted that the K_{sec} key is an asymmetric key between S_i and *SS*, on the one hand, and on the other hand initialized out of band by the latter, it makes it possible to guarantee the secure transmission of the symmetric key K_{msg} which will be used for regular communications, it is therefore, the low frequency of use of this key which protects it against cryptanalysis. Also, we assume that the connection between BNC and SS is secured.

The initial connection requires the connection between BNC and SS, it then becomes important, but not essential, because the regular frequency refresh (using *RC*) of the key is one of the mechanisms to enhance the security of the proposed solution, but it is still possible that the connection may be impossible or interrupted in some cases. To remedy this, the solution plans to continue using the same K_{msg} key until a new key has been obtained.

The renewal mechanism is based on the fact that the primary interest of such a system is the possibility of remote and permanent monitoring of persons with a BAN, and takes advantage of this permanent link to enhance the security of the BAN, but it does not exclude the hazards of a wide area network and therefore provides for measures to ensure the continuity of the functioning of the BAN.

The renewal of the K_{msg} key is planned by the BNC during the distribution of each key; it defines a certain number of cycles (Superframe) before renewing the key. This involves finding a compromise between encryption resilience and sensor computing capabilities to determine the optimal update time and the time-lapse beyond which security can be compromised, and the same goes for K_{sec} through using an out-of-band method as planned during the initialization process.

7.3 SBSKM performances evaluation:

As we detailed previously, our solution includes, in addition to the sensors and the BNC that exists in the standard architecture, a security server; it acts as a trusted server to which the BNC is connected. It is responsible for initializing and resetting the K_{sec} keys of the sensors, and is responsible for ensuring their identity, in addition to renewing the K_{msg} keys used.

It, therefore, meets the need for a trusted authority to certify sensor identities to respond to the risks of Sybil attacks, besides, the server manages key renewals and therefore protects against cryptanalysis attempts.

- **Initialization phase:**

The standard introduces the concept of initialization into the connection process when generating the MK key in the association process (Protocol I, II, III, IV), the standard also envisages the use of pre-shared keys (Protocol II) and secret passwords (Protocol III).However, the standard does not specify a method for this initialization apart from the fact that it occurs in out-of-band, and does not propose a solution to the MK key generation process that occurs in clear, nor to the renewal of secret and public keys (PK_x, PK_y and SK) of sensors and BNCs, which are therefore vulnerable.

Our solution uses the principle of key initialization, but by improving its reliability, because this time the security server is responsible for the out-of-band transmission of the initial keys, moreover they are unique for each sensor, and renewable if necessary, so they encrypt communications from the beginning and are renewable to counter cryptanalysis attacks.

- **Connection phase:**

The security association provided by the standard is based on the auto-generation of MKs keys (type ECC-128) which creates vulnerability because of the packets sent in clear during the generation of the key, leading to the possible compromise of the generated key.

Our solution protects itself from this vulnerability by using a strong renewable key system (RSA-1024) initiated out of band, and a trusted server to guarantee the identity of the sensors from the beginning of the connection process. This system also allows to better protect the key used later for communications (K_{msg}) of type AES-128 during its transmission to the sensor.

It is also important to note that the connection process of our solution generates only two (02) encrypted communications (from the sensor), one incoming and one outgoing instead of four (04) unencrypted communications in the standard, which reduces the number of communications that can be intercepted by an attacker and the ease of analyzing its content.

- **Communications:**

Our solution, like the standard, encrypts all its communications using an encryption algorithm that combines reduced encryption time, strength, and energy savings with the AES-128 algorithm. The standard also uses a PTK key equivalent to AES-128[17] for these communications, so we consider that SBSKM remains equivalent to the standard in this respect.

Our solution adds to this the possibility of periodically renewing the encryption key after a certain number of Superframes at the initiative of the BNC, thus guaranteeing better protection against cryptanalysis.

7.3.1 Results and Interpretation:

- **Simulation parameters:**

To show the effectiveness of the proposed scheme, we will compare the SBSKM performances with the unsecured IEEE 802.15.6 and the IEEE 802.15.6 with Security Association (SA). As shown in the literature, the key management fulfills the security requirements of the target network and also resists against various security attacks such as impersonation attacks [15]. It remains to assess the impact of the SBSKM on network performances such as the number of received packets by the BNC, the energy consumption,

the latency, and the failure rate of packets. To evaluate our proposal, we configured a WBAN as in Table 15:

Network Settings	
Access scheme	CSMA/CA
Number of nodes	12
Simulation time (second)	501s (50 repetitions)
Slot allocation length (ms)	10
MAC Buffer	100 packets
Retransmission packets tries	2
Phy Layer overhead (Bytes)	6
Mac frame overhead (Bytes)	7
Packet header overhead (Bytes)	5
Data payload (Bytes)	100
Mobility of nodes	No.
Arrival rate (p/s)	1, 4, 8, 16, 32, 64, 80, 100

Table 15: Simulation Network Settings

To make the simulation as realistic as possible, we used the radio transmitters proposed by the simulator and compatible with the parameters of the standards, the characteristics of the radio are as follows:

Radio Settings	
Data rate (kbps)	1024
Modulation Type	DIFFQPSK
Bits Per Symbol	2
Bandwidth (MHz)	20
Noise Bandwidth (MHz)	1000
Noise Floor (dBm)	-104
Sensitivity (dBm)	-87
Power Consumed on reception mode (mW)	3.1
transmission power (dBm)	-15
Power Consumed on transmission mode (mW)	2.93
Power consumed on transition (transmission, reception) (mW)	3
Time of transition (transmission, reception)	0.02

Table 16: Radio parameters of the security simulation

The processing delays and energy costs of the security tasks for the IEEE 802.15.6 standard using Diffie-Hellman encryption (ECC-160) and for our solution using RSA-1024 and AES-128 were taken from calculated parameters on sensor nodes that can be used in WBANs (MICA2DOT)[59],[57],[75]. A summary of the security parameters is shown in Table 17.

Parameters Model	SBSKM	IEEE 802.15.6 with SA
Initialization	RSA-1024	ECC-160
Connection time	2980 ms	1650 ms
Energy Consumption	32.67 mWs	54.46 mWs

Communications	AES-128 Encrypt / decrypt	Camellia-128 Encrypt / decrypt
Time	2.14 ms	2 ms
Energy Consumption	23.85 µWs	19.8 µWs

Table 17: Simulation parameters of the SBSKM and IEEE 802.15.6

It is important to note that only exchanges between sensor nodes and the BNC are taken into account; communications between the BNC and the SS in our solution will be introduced into our simulations as BNC-specific processing.

7.3.2 Analysis of the results:

The parameters we evaluated during the simulations of the three models were the number of packets received by the BNC, sensor energy consumption, transmission quality and latency. At the end of the simulations, we obtained the following results:

a. The number of packets received by the BNC:

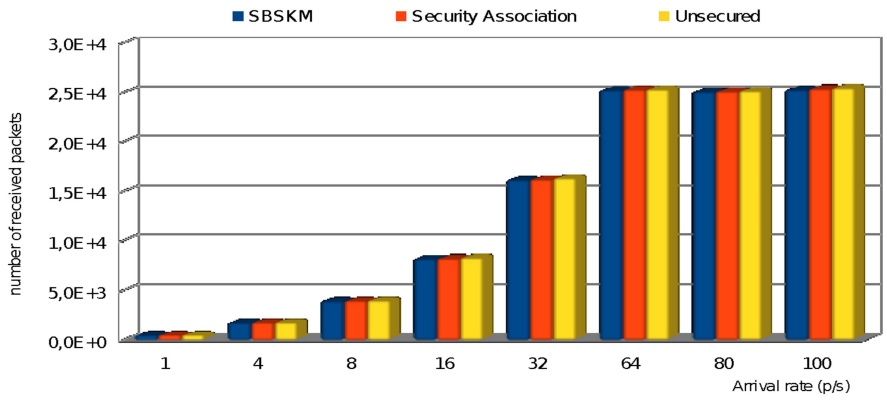

Figure 66: Total number of packets received by the BNC

We notice from Figure 66 that the number of packets received by the BNC is approximately the same for all three models. We notice also that the highest number of received packets is of the unsecured model because unlike other models, the nodes in this model use the encryption, decryption, and the initialization times to send packets to the BNC. The lowest number of received packets is achieved by the model using the SBSKM protocol because of the importance of the processing time required for encryption at all steps. We remark also that from 64 p/s, the three models seem to reach a maximum limit of received packets. This is explained by the saturation of the transmission channel and the saturation of the MAC queue, which results in packets dropping.

b. Energy consumption:

This graph describing the energy consumption of the security process gives us a better idea of the difference between the SBSKM model and IEEE 802.15.6. Indeed, in Figure 67, the IEEE 802.15.6 with SA seems to be more energy-consuming than for the SBSKM model at a low packet arrival rate because the initialization consumption energy is higher in the first model. While, by increasing the arrival rate, this difference is quickly reversed by the SBSKM model, which is more energy-consuming on encryption and decryption operations. It should be noticed that despite the stability of the number of packets received by the BNC, the energy consumption continues to increase with the increase of packets' arrival rate because packets are only ignored at the MAC layer after that they have been encrypted at the application layer. For the overall energy consumption, described in Figure 68, the same observation is made for the energy consumption of the security process between the IEEE 802.16.6 with SA and SBSKM. In addition to that, the fact that the energy consumption of the unsecured IEEE 802.15.6 model decreases slightly with the increase in the arrival rate is because the sensors consume more energy during active listening than during sending, as indicated in Table 16.

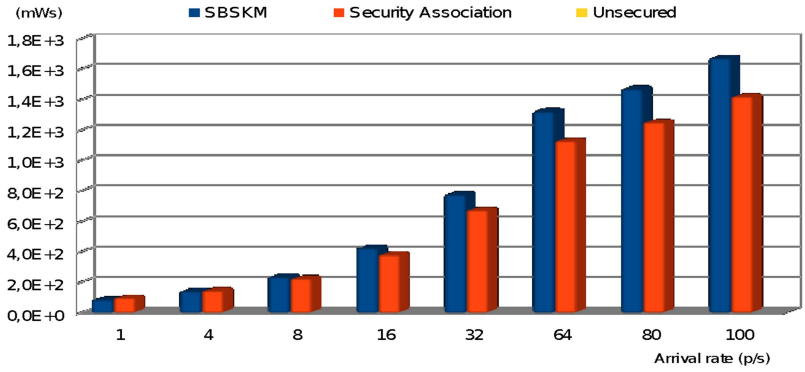

Figure 67: Energy consumption in (mWs) in the security process

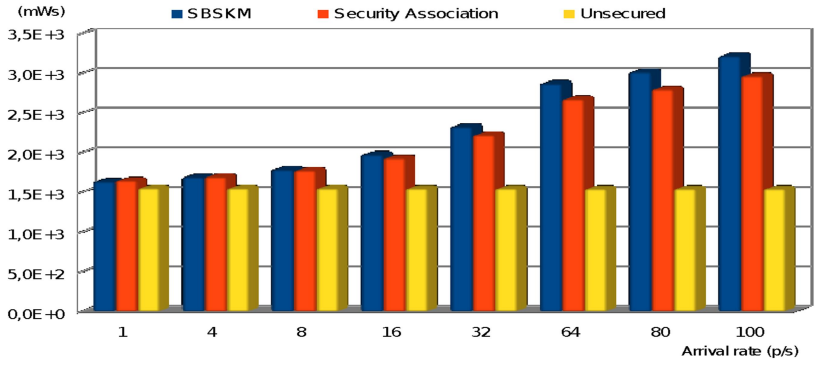

Figure 68: Total energy consumption in (mWs) in the WBAN

c. The failure rate of the transmissions:

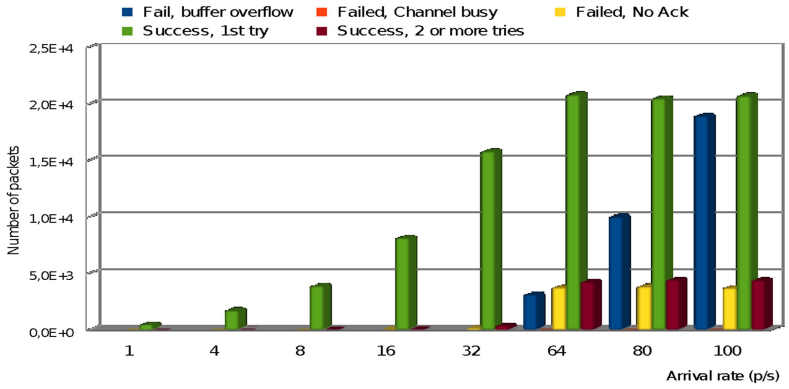

Figure 69: Packet failure rate for the SBSKM protocol

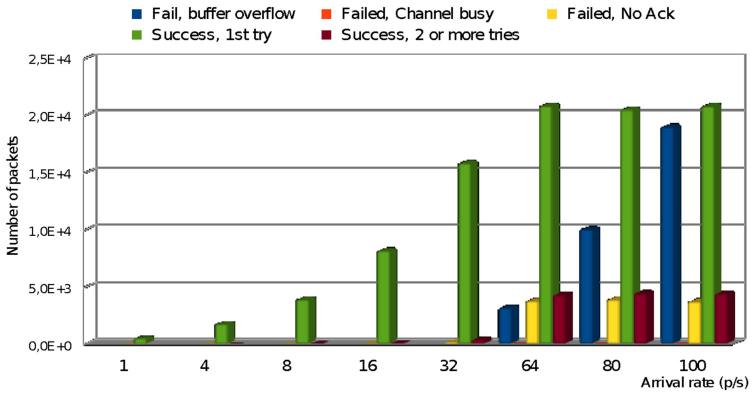

Figure 70: Packet failure rate for IEEE 802.15.6 with SA

As shown in figures 69 and 70, the failure rates, corresponding to the SBSKM and IEEE 802.15.6 with SA models, are almost identical, proof that the slight differences in encryption times by the used algorithms do not have an impact on the overall failure rate of the transmissions. It is also noticeable that from 64 p/s both models will reach the medium use saturation. This results in an increase in the number of failed transmissions due to buffer overflow, while the number of successful transmissions will remain steady.

d. Latency:

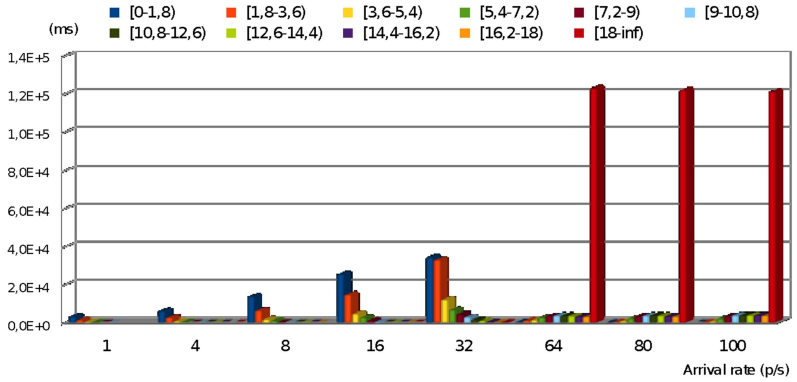

Figure 71: Latency in (ms) for the unsecured IEEE 802.15.6.

Figure 71represents the latency of the unsecured IEEE 802.15.6 model, which is the delay elapsed from the moment of packets' generation until their successful transmission or their drop. We immediately notice that from 64 p/s, almost all communications have a latency greater than 18 ms. This, according to what has been explained before, is due to the combined effect of the channel saturation and the waiting time in the MAC queue.

The following two graphs, shown in figures 72 and 73, represent the latency for the SBSKM and the IEEE 802.15.6 with SA models. On the first hand, we notice that the two models have the same behavior regarding the latency. On the other hand, there is a high similarity between these two graphs and the previous one, in terms of shape and values. This can lead us to conclude that securing the standard by both methods practically does not disrupt the initial performance of the network, which remains limited only by its physical characteristics of sensor nodes.

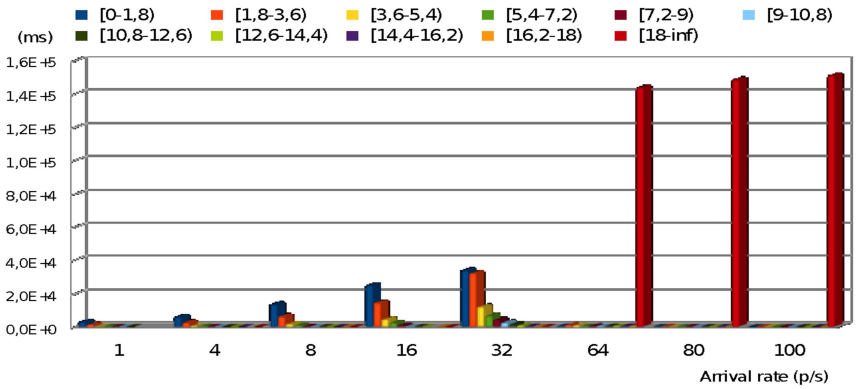

Figure 72: Latency in (ms) for the SBSKM protocol

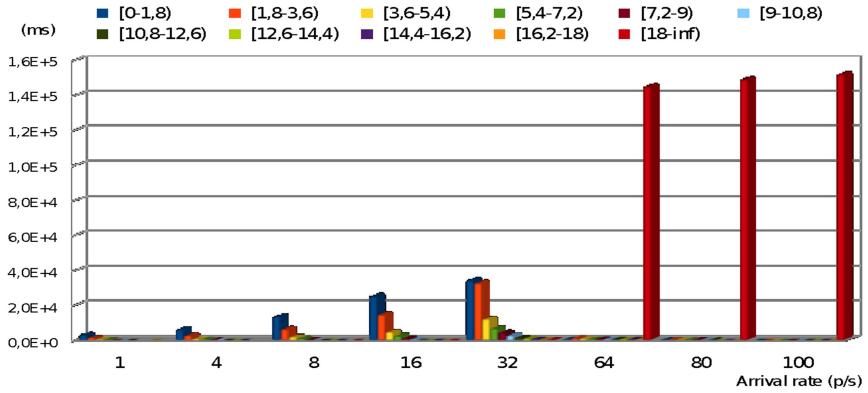

Figure 73: Latency in (ms) for the IEEE 802.15.6 with SA

- **Key renewal for the SBSKM model:**

We vary in this simulation the number of the K_{msg} renewals for 500 seconds. This is not necessarily admissible in real applications due to the robustness of the used security key, but our objective is to show the impact of the renewal operation on the overall performance of the network. We kept all simulation parameters unchanged as in the previous simulations except the number of generated packets which set to 25 p/s. We notice from Figure 74 that the number of received packets at the BNC decreases with the increase of the frequency of key renewal. This is due mainly to the interruption of sending packets during the key renewal phase. To show the difference between the three cases, we start the x-axis in the following Figure from 11,900 packets instead of zero. This justifies the deviation between the three presented cases.

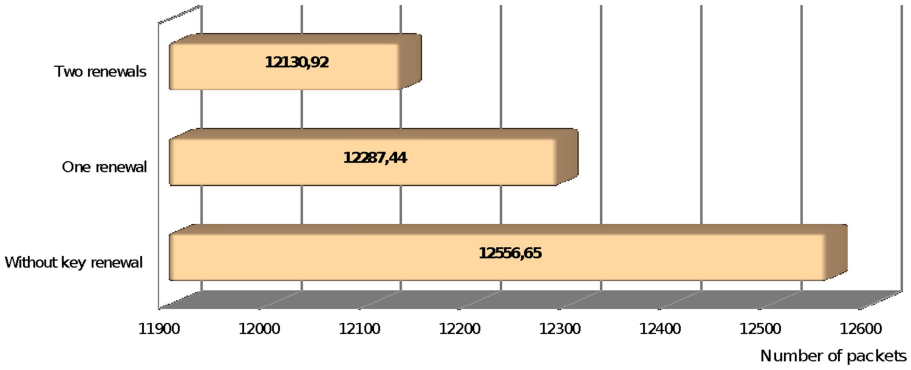

Figure 74: The average number of packets received by the BNC

We remark from Figure 75 that energy consumption increases significantly with the increase in the number of renewals and reaches 737.52 mWs. This is due mainly to the amount of energy consumed during the key renewal process.

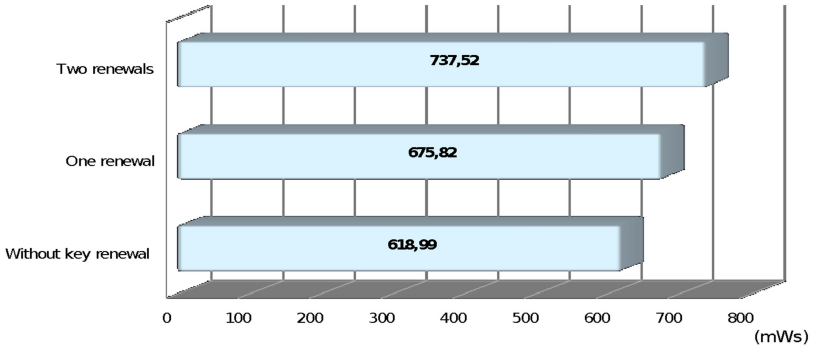

Figure 75: Total energy consumption in (mWs) for key renewal

quality of transmissions in the network, as shown in Figure 76, does not differ significantly, except for the number of packets received by the BNC which was previously processed, the number of abandoned packets, and the number of successful transmissions after the second or more attempts remain relatively unchanged because the data sending rate remains within physical reach for the nodes.

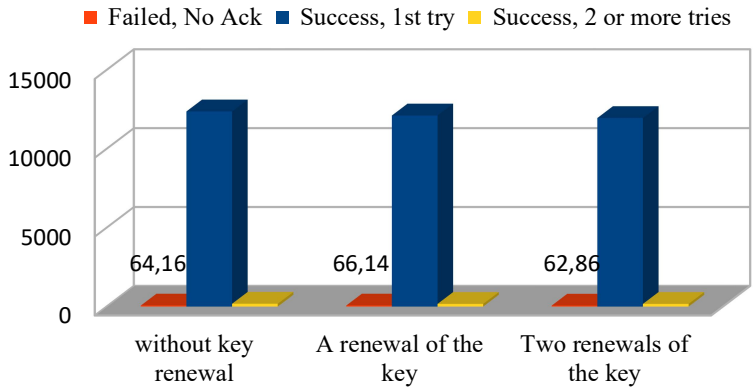

Figure 76: Packet failure rate at the MAC layer

Although the above figures show a slight influence of the key renewal process on the overall performance of WBANs, its impact will remain insignificant in real situations where renewal is not as frequent as in simulations.

7.4 Conclusion

By studying the security mechanisms proposed by the IEEE 802.15.6 standard in chapter 3,we highlighted the strengths as well as the weaknesses of these mechanisms, in particular the point related to the vulnerability to the impersonation attack. To address such vulnerability, we have designed a Server-Based Secure Key Management for the IEEE 802.15.6 standard protocol. Simulation results showed the effectiveness of the proposed solution which allowed

us to overcome the lack of authentication and confidentiality in the standard security scheme and deal with the impersonation attacks without affecting the standard's performances.

8 CONCLUSION AND FUTURE DIRECTIONS

A WBAN is a wireless network of several miniature biosensors that can be implanted inside the body, mounted on the body's surface, or a device that can be worn in clothing pockets, by hand, or in various bags. WBANs have gained much interest and became emerging technology in health monitoring due to its wide range of use in improving human health. Many earlier wireless technologies were used for the transport of medical data both to and from medical devices but these standards were not appropriate for wireless communication around the human body. The first international WBANs standard was established by the Task Group 6 and called IEEE 802.15.6. Many evaluations and studies were conducted to study the standard performances and show their strengths and weaknesses. In the same context, in this thesis, our main focus was to study the unaddressed aspects of the standard such as the QoS and security, and provide more performance evaluation over simulation and analytical models. We first introduced the necessary background information to understand the presented research work, starting from the WBANs environment. Afterward, we focus on the IEEE 802.15.6 standard. Therefore, we presented a general overview of the standard, and subsequently, we highlight the issues and challenges that motivated the work presented in this thesis. After that we presented our main contributions, starting with two performance evaluation contributions of the standard. The first one concerns a simulation analysis of the standard in a real medical scenario to show its effectiveness in critical healthcare applications. The second evaluation deals with queueing strategies and their impact to guarantee a high QoS for emergency traffic. In our main contribution, we provided a general and accurate analytical model allowing the study of the IEEE 802.15.6 CSMA/CA access scheme, in terms of latency and packets breakdown at the MAC layer while assuming that sensor nodes can generate heterogeneous traffic in term of priority. The last contribution proposes a protocol called Server-Based Secure Key Management (SBSKM), which takes up the principle of the trusted server, by introducing some tasks and procedures to be supported on this server as well as on the BNC and sensors. The proposed solution aims to reinforce the security established by the IEEE 802.15.6 standard, by trying to overcome the proven vulnerabilities of the latter.

Open Issues and Future Directions:

Future perspectives for our work can encompass several directions, As the first challenge is to analyze the IEEE 802.15.6 based WBANs with an M/ G/1/k non-preemptive priority in which MAC buffers are limited in length and extend the proposed analytical model to handle packets length variation and the Ack frame failing transmission. The renewal reward modeling approach can also be extended to analyze networks with non-saturated conditions and channel fading and shadowing caused by communication around the human body. Another interesting topic to tackle is to explore more complicated ISO/IEEE 11073 use cases to evaluate the behavior of the standard, the coexistence of WBANs and the interferences issues, and how we can mitigate their impacts. Moreover, security is another perspective to address. We provided in this thesis a framework to deal with the impersonation attacks whereas many other attacks need to be addressed and taken into account by proposing a more comprehensive solution.

Bibliography:

[1] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wirel. Networks*, vol. 17, no. 1, pp. 1–18, Jan. 2011.

[2] IEEE, "IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-1997*, pp. i–445, 1997.

[3] IEEE, *IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements*, no. June. IEEE, 2002.

[4] IEEE, "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements–Part 15.4: Wireless MAC and PHY Specifications for Low-Rate WPANs," IEEE, 2006.

[5] IEEE Standards Association, *IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks*, no. February. 2012.

[6] R. Huang, Z. Nie, C. Duan, Y. Liu, L. Jia, and L. Wang, "Analysis and Comparison of the IEEE 802.15.4 and 802.15.6 Wireless Standards Based on MAC Layer," in *Health Information Science*, vol. 9085, Springer International Publishing, 2015, pp. 7–16.

[7] IEEE Standards Association, "IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks," *IEEE Std*, no. February, p. 271, 2012.

[8] S. Rashwand, J. Misic, and V. B. Misic, "Analysis of CSMA/CA Mechanism of IEEE 802.15.6 under Non-Saturation Regime," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 5, pp. 1279–1288, 2016.

[9] S. Sarkar, S. Misra, B. Bandyopadhyay, C. Chakraborty, and M. S. Obaidat, "Performance analysis of IEEE 802.15.6 mac protocol under non-ideal channel conditions and saturated traffic regime," *IEEE Transactions on Computers*, vol. 64, no. 10. pp. 2912–2925, 2015.

[10] M. S. Chowdhury, P. Khan, J. Jung, and K. S. Kwak, "Modeling Slotted Aloha of WBAN in non-saturated conditions," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 6, pp. 1901–1913, 2014.

[11] P. Khan, N. Ullah, and H. Kim, "WBAN MAC protocols— Non-saturation modeling and performance analysis," *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 3, pp. 1462–1476, Mar. 2017.

[12] A. Mukherjee, B. Bandyopadhyay, D. Das, A. Chatterjee, S. J. Ahmed, and M. Naskar, "Markov chain based analysis of IEEE 802.15.6 MAC protocol in real life scenario," in *Proceedings of the 9th International Conference on Body Area Networks*, 2014, pp. 331–337.

[13] A. K. Jacob, G. M. Kishore, and L. Jacob, "Lifetime and latency analysis of IEEE 802.15.6 WBAN with interrupted sleep mechanism," *Sādhanā*, vol. 42, no. 6, pp. 865–878.

[14] D. T. Quan, P. T. Hiep, and R. Kohno, “Performance Analysis Method for IEEE 802.15.6 Based WBANs with Adaptive BCH Code Rates,” *Wirel. Pers. Commun.*, vol. 94, no. 3, pp. 605–619, Jun. 2017.

[15] S. Ullah, E. Tovar, K.-I. Kim, K. H. Kim, and M. Imran, “Performance Analysis of Priority-Based IEEE 802.15.6 Protocol in Saturated Traffic Conditions,” *IEEE Access*, pp. 1–1, 2018.

[16] T. Benmansour, T. Ahmed, and S. Moussaoui, “Performance Evaluation of IEEE 802.15.6 MAC in Monitoring of a Cardiac Patient,” in *Proceedings - Conference on Local Computer Networks, LCN*, 2016.

[17] T. Benmansour, T. Ahmed, and S. Moussaoui, “Performance analyses and improvement of the IEEE 802.15.6 CSMA/CA using the low latency queuing,” in *2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2017, pp. 1–6.

[18] T. Benmansour, T. Ahmed, S. Moussaoui, and Z. Doukha, “Performance analyses of the IEEE 802.15.6 wireless body area network with heterogeneous traffic,” *J. Netw. Comput. Appl.*, p. 102651, Apr. 2020.

[19] T. Benmansour, S. Moussaoui, T. Ahmed, and O. Boutaghou, “Server-Based Secure Key Management for the IEEE 802.15.6 standard,” in *2020 IEEE Symposium on Computers and Communications (ISCC)*, 2020, pp. 1–6.

[20] M. Alam and E. Hamida, “Surveying Wearable Human Assistive Technology for Life and Safety Critical Applications: Standards, Challenges and Opportunities,” *Sensors*, vol. 14, no. 5, pp. 9153–9209, May 2014.

[21] M. Li and M. Zhuang, “An overview of Physical layers on wireless body area network,” in *Anti-counterfeiting, Security, and Identification*, 2012, pp. 1–5.

[22] T. Benmansour, T. Ahmed, and S. Moussaoui, “Performance Evaluation of IEEE 802.15.6 MAC in Monitoring of a Cardiac Patient,” in *2016 IEEE 41st Conference on Local Computer Networks Workshops (LCN Workshops)*, 2016, pp. 241–247.

[23] N. Bradai, L. C. Fourati, and L. Kamoun, “Investigation and performance analysis of MAC protocols for WBAN networks,” *J. Netw. Comput. Appl.*, vol. 46, pp. 362–373, Nov. 2014.

[24] A. Nabila and E. B. Mohamed, “A QoS based comparative analysis of the IEEE standards 802.15.4 & 802.15.6 in WBAN-based healthcare monitoring systems,” in *2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*, 2019, pp. 1–5.

[25] A. Natarajan, B. de Silva, K.-K. Yap, and M. Motani, “To Hop or Not to Hop: Network Architecture for Body Sensor Networks,” in *2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2009, pp. 1–9.

[26] S. Ullah *et al.*, “A comprehensive survey of wireless body area networks on PHY, MAC, and network layers solutions,” *J. Med. Syst.*, vol. 36, no. 3, pp. 1065–1094, Jun. 2012.

[27] G. Lazzi, “Thermal effects of bioimplants,” *IEEE Eng. Med. Biol. Mag.*, vol. 24, no. 5, pp. 75–81, Sep. 2005.

[28] M. Al Ameen, J. Liu, and K. Kwak, “Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications,” *J. Med. Syst.*, vol. 36, no. 1, pp. 93–101, Feb. 2012.

[29] P. Niksaz, “Wireless Body Area Networks: Attacks and Countermeasures,” *Int. J. Sci. Eng. Res.*, vol. 6, no. 9, 2015.

[30] S. Saleem, S. Ullah, and K. S. Kwak, “A study of IEEE 802.15.4 security framework for wireless body area networks,” *Sensors*, vol. 11, no. 2, pp. 1383–1395, Feb. 2011.

[31] Y. Wang, G. Attebury, and B. Ramamurthy, “A survey of security issues in wireless sensor networks,” *IEEE Communications Surveys and Tutorials*, vol. 8, no. 2. pp. 2–22, Jun-2006.

[32] J. Chen and H. L. Zhang, “Survey on wireless sensor network security,” *Harbin Gongye Daxue Xuebao/Journal Harbin Inst. Technol.*, vol. 43, no. 7, pp. 90–95, Jul. 2011.

[33] K. ur R. R. S. Muhammad, H. Lee, S. Lee, and Y. K. Lee, “BARI+: A biometric based distributed key management approach for wireless body area networks,” *Sensors*, vol. 10, no. 4, pp. 3911–3933, Apr. 2010.

[34] V. Sivaprasatham and J. Venkateswaran, “A secure key management technique for wireless body area networks,” *J. Comput. Sci.*, vol. 8, no. 11, pp. 1780–1787, 2012.

[35] A. Salam, A. Nadeem, K. Ahsan, M. Sarim, and K. Rizwan, “A class based QoS model for Wireless Body Area Sensor Networks,” *Res. J. Recent Sci.*, vol. 3, no. 7, pp. 69–78, 2014.

[36] C. Kateretse, G.-W. Lee, and E.-N. Huh, “A Practical Traffic Scheduling Scheme for Differentiated Services of Healthcare Systems on Wireless Sensor Networks,” *Wirel. Pers. Commun.*, vol. 71, no. 2, pp. 909–927, Jul. 2013.

[37] M. Iftikhar, N. Al Elaiwi, and M. S. Aksoy, “Performance Analysis of Priority Queuing Model for Low Power Wireless Body Area Networks (WBANs),” *Procedia Comput. Sci.*, vol. 34, pp. 518–525, 2014.

[38] S. Rashwand and J. Mišić, “Effects of access phases lengths on performance of IEEE 802.15.6 CSMA/CA,” *Comput. Networks*, vol. 56, no. 12, pp. 2832–2846, 2012.

[39] C. Li, X. Geng, J. Yuan, and T. Sun, “Performance analysis of IEEE 802.15.6 MAC protocol in beacon mode with superframes,” *KSII Trans. Internet Inf. Syst.*, vol. 7, no. 5, pp. 1108–1130, 2013.

[40] M. Fatehy and R. Kohno, “A novel contention probability dynamism for IEEE 802.15.6 standard,” *EURASIP J. Wirel. Commun. Netw.*, vol. 2014, no. 1, p. 92, 2014.

[41] A. Muthulakshmi and K. Shyamala, “Queuing Based Emergency Handling in,” vol. 7, no. 6, pp. 2231–2239, 2016.

[42] V. Marbukh, M. Barbi, K. Sayrafian, and M. Alasti, “A queue-size & channel

quality based adaptation of the energy detection threshold in IEEE802.15.6 CSMA/CA," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 2016, pp. 1–6.

[43] J. Ghaderi and R. Srikant, "The Impact of Access Probabilities on the Delay Performance of Q-CSMA Algorithms in Wireless Networks," *IEEE/ACM Trans. Netw.*, vol. 21, no. 4, pp. 1063–1075, Aug. 2013.

[44] C. Yi, A. S. Alfa, and J. Cai, "An Incentive-Compatible Mechanism for Transmission Scheduling of Delay-Sensitive Medical Packets in E-Health Networks," *IEEE Trans. Mob. Comput.*, vol. 15, no. 10, pp. 2424–2436, Oct. 2016.

[45] C. Yi and J. Cai, "A Priority-Aware Truthful Mechanism for Supporting Multi-Class Delay-Sensitive Medical Packet Transmissions in E-Health Networks," *IEEE Trans. Mob. Comput.*, vol. 16, no. 9, pp. 2422–2435, Sep. 2017.

[46] S. Rashwand and J. Misic, "Two-tier WBAN/WLAN healthcare networks; Priority considerations," in *GLOBECOM - IEEE Global Telecommunications Conference*, 2012, pp. 5398–5403.

[47] G. Bianchi, "IEEE 802.11 - Saturation throughput analysis," *IEEE Commun. Lett.*, vol. 2, no. 12, pp. 318–320, Dec. 1998.

[48] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535–547, Mar. 2000.

[49] S. Rashwand, J. Mišić, and H. Khazaei, "IEEE 802.15.6 under saturation: Some problems to be expected," *J. Commun. Networks*, vol. 13, no. 2, pp. 142–148, 2011.

[50] S. Rashwand, J. Mišić, and H. Khazaei, "Performance analysis of IEEE 802.15.6 under saturation condition and error-prone channel," *2011 IEEE Wirel. Commun. Netw. Conf. WCNC 2011*, pp. 1167–1172, 2011.

[51] M. S. Chowdhury, K. Ashrafuzzaman, and K. S. Kwak, "Saturation throughput analysis of IEEE 802.15.6 slotted aloha in heterogeneous conditions," *IEEE Wirel. Commun. Lett.*, vol. 3, no. 3, pp. 257–260, 2014.

[52] P. Khan *et al.*, "Performance analysis of different backoff algorithms for WBAN-based emerging sensor networks," *Sensors (Switzerland)*, vol. 17, no. 3, p. 492, Mar. 2017.

[53] H. Fourati, H. Idoudi, and L. A. Saidane, "Intelligent slots allocation for dynamic differentiation in IEEE 802.15.6 CSMA/CA," *Ad Hoc Networks*, vol. 72, pp. 27–43, Apr. 2018.

[54] K. S. Deepak and A. V. Babu, "Improving reliability of emergency data frame transmission in IEEE 802.15.6 wireless body area networks," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2082–2093, Sep. 2018.

[55] H. Yu, L. Fu, and Y. Xu, "Unified fixed-point analysis of IEEE 802.11 WLAN under saturated and unsaturated conditions," *Wirel. Commun. Mob. Comput.*, vol. 12, no. 7, pp. 588–597, May 2012.

[56] Xinhua Ling, Yu Cheng, J. W. Mark, and Xuemin Shen, "A Renewal Theory Based Analytical Model for the Contention Access Period of IEEE 802.15.4 MAC," *IEEE*

Trans. Wirel. Commun., vol. 7, no. 6, pp. 2340–2349, Jun. 2008.

[57] M. Toorani, "Security analysis of the IEEE 802.15.6 standard," *Int. J. Commun. Syst.*, vol. 29, no. 17, pp. 2471–2489, Nov. 2016.

[58] S. Ullah, M. Mohaisen, and M. A. Alnuem, "A review of IEEE 802.15.6 MAC, PHY, and security specifications," *Int. J. Distrib. Sens. Networks*, vol. 2013, no. February, pp. 0–13, 2013.

[59] M. Toorani, "On vulnerabilities of the security association in the IEEE 802.15.6 standard," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8976, pp. 245–260, 2015.

[60] E. Engineers, T. P. Avenue, S. Licensing, and S. Licensing, "Draft Standard for Health informatics - Point-of-care medical device communication - Nomenclature - Implantable device , cardiac," vol. 4, no. January, 2005.

[61] "Unapproved IEEE Draft Guide for Health Informaticspoint-Of-Care Medical Device Communicationtechnical Reportguidelines for the Use of RF Wireless Technology," *IEEE Std P1073.0.1.1/D01J*, p. , 2006.

[62] NICTA, "Castalia Simulator," 2011. [Online]. Available: https://castalia.forge.nicta.com.au/index.php/en/. [Accessed: 21-Nov-2015].

[63] TEXAS INTRUMENTS, "CC2420," 2006. [Online]. Available: http://www.ti.com/product/CC2420. [Accessed: 16-Mar-2016].

[64] P. Denise M. Bevilacqua Masi, P. Martin J. Fischer, and David A. Garbin, "MODELING THE PERFORMANCE OF LOW LATENCY QUEUEING FOR EMERGENCY TELECOMMUNICATIONS."

[65] V. G. Kulkarni, *Introduction to Modeling and Analysis of Stochastic Systems*. Chapman & Hall, 2011.

[66] "- Document - Probability, Stochastic Processes, and Queueing Theory: The Mathematics of Computer Performance Modeling." [Online]. Available: https://go.galegroup.com/ps/anonymous?id=GALE%7CA18586301&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=01621459&p=AONE&sw=w. [Accessed: 02-Nov-2019].

[67] S. Ullah, M. Chen, and K. S. Kwak, "Throughput and delay analysis of IEEE 802.15.6-based CSMA/CA protocol," *J. Med. Syst.*, vol. 36, no. 6, pp. 3875–3891, 2012.

[68] Z. Papir, "Queueing Theory with Applications to Packet Telecommunications [Book Review]," *IEEE Commun. Mag.*, vol. 44, no. 5, pp. 2005–2006, 2005.

[69] M. Veeraraghavan, "Priority queueing (nonpreemptive)," vol. 1, no. Eq 2, pp. 1–8, 2004.

[70] I. Adan, *Queueing theory : Ivo Adan and Jacques Resing.* Eindhoven: Eindhoven University of Technology. Department of Mathematics and Computing Science, 2001.

[71] J. B. M. Doremalen, "A mean-value approach for M/G/1 priority queues," 1983.

[72] J. D. C. Little, "A Proof for the Queuing Formula: L = λ W," *Oper. Res.*, vol. 9, no. 3,

pp. 383–387, Jun. 1961.

[73] R. W. Wolff, “Poisson Arrivals See Time Averages,” *Oper. Res.*, vol. 30, no. 2, pp. 223–231, Apr. 1982.

[74] X. Ling, Y. Cheng, J. W. Mark, and X. Shen, “A renewal theory based analytical model for the contention access period of IEEE 802.15.4 MAC,” *IEEE Trans. Wirel. Commun.*, vol. 7, no. 6, pp. 2340–2349, 2008.

[75] P. Trakadas, T. Zahariadis, H. C. Leligou, S. Voliotis, and K. Papadopoulos, “Analyzing energy and time overhead of security mechanisms in wireless sensor networks,” in *Proceedings of IWSSIP 2008 - 15th International Conference on Systems, Signals and Image Processing*, 2008, pp. 137–140.