Contributions to the energy optimization for security, localization and routing in wireless sensor networks

Anouar Abdelhakim Boudhir

To cite this version:

Anouar Abdelhakim Boudhir. Contributions to the energy optimization for security, localization and routing in wireless sensor networks. Networking and Internet Architecture [cs.NI]. Université Abdelmalek Essaâdi; Faculté des Sciences et Technique de Tanger, 2013. English. NNT : . tel-00830885

HAL Id: tel-00830885

https://theses.hal.science/tel-00830885

Submitted on 5 Jun 2013

N° d'ordre : 72 Année : 2012 / 2013

جامعة عبد المالك السعدي
Université Abdelmalek Essaadi

UNIVERSITE ABDELMALEK ESSAADI
FACULTE DES SCIENCES et TECHNIQUES
TANGER

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

THESE DE DOCTORAT

Présentée

Pour l'obtention du

DOCTORAT EN SCIENCES ET TECHNIQUES DE L'INGENIEUR

Par :
Anouar Abdelhakim BOUDHIR

Discipline : Informatique et Télécommunication

Spécialité : Réseaux, Informatique et Télécommunication

Titre de la Thèse : Contributions à l'optimisation de l'énergie pour la sécurité, la localisation et le routage dans les réseaux de capteurs sans fil.

Soutenue le 11 Mai 2013 devant le Jury :

Pr. OTMAN FILALI MEKNASSI	Ecole Nationale des Sciences Appliquées de Tanger	**Président**
Pr. FATTEHALLAH GHADI	Vice Président de l'Université IBN ZOHR d'Agadir	**Rapporteur**
Pr. MOHAMMED BOULMALF	Université Internationale de Rabat	**Rapporteur**
Pr. ABDELALI ASTITO	Faculté des Sciences et Techniques de Tanger	**Rapporteur**
Pr. MOHAMMAD AL-TURKISTANY	Umm Al-Qura University of Makkah	**Examinateur**
Pr. MOHAMMED BOUHORMA	Faculté des Sciences et Techniques de Tanger	**Directeur de Thèse**

Structure de recherche accréditée d'accueil :
Laboratoire d'Informatique et Systèmes de Télécommunication **de la FST de Tanger (UAE/L08)**

Serial Number : 72 Year : 2012 / 2013

جامعة عبد المالك السعدي
Université Abdelmalek Essaadi

ABDELMALEK ESSAADI UNIVERSITY
FACULTY OF SCIENCES AND TECHNIQUES TANGIER

Doctoral Studies Center: « Science and Technology Engineer»
Doctoral training: « Science and Technology Engineer»

DOCTORAL THESIS

Presented

To obtain the

DOCTOR OF SCIENCES AND ENGINEERING TECHNIQUES

By:

Anouar Abdelhakim BOUDHIR

Discipline: Computer Sciences and Telecommunications
Specialty: Networks, Computer Sciences and Telecommunications

Thesis Title: Contributions to the energy optimization for security, localization and routing in wireless sensor networks.

Sustained May 11, 2013 in front of the jury:

Pr. OTMAN FILALI MEKNASSI	National School of Applied Sciences of Tangier	**President**
Pr. FATTEHALLAH GHADI	Vice President of the University IBN ZOHR of Agadir	**Reporter**
Pr. MOHAMMED BOULMALF	International University of Rabat	**Reporter**
Pr. ABDELALI ASTITO	Faculty of Sciences and Techniques of Tangier	**Reporter**
Pr. MOHAMMAD AL-TURKISTANY	Umm Al-Qura University of Makkah	**Examiner**
Pr. MOHAMMED BOUHORMA	Faculty of Sciences and Techniques of Tangier	**Thesis director**

Accredited Structure Of Research:
Laboratory of Computer and Telecommunication Systems of the FST of Tangier (UAE/L08)

بسم الله الرحمن الرحيم

{وَقَلِ اعْمَلَوا فَسَيَرَى اللّهُ عَمَلَكَمْ وَرَسُولهُ وَالمُؤْمِنُونَ}

105 التوبة

{وَمَا أُوتِيتُمْ مِنَ العِلْمِ إِلاّ قَلِيلاً}

الإسراء85

صدق الله العظيم

Remerciements

Dans un premier temps, je n'ai qu' adresser un grand merci à Dieu, le tout puissant, qui nous guide et nous éclaire la voie et le chemin droit, je le remercie encore de m'avoir permis d'emprunter le chemin de la recherche en s'inscrivant en master de recherche (SIR) Systèmes Informatiques et Réseaux de la FST de Tanger. Je n'aurais sans doute pas fait de thèse si je n'avais pas suivi cette formation. Je tien donc à remercier le Professeur BOUHORMA Mohamed à double titre, pour avoir dirigé avec succès cette formation, et pour m'avoir fait l'honneur de diriger ma thèse. Son soutien, ses directives et instructions m'ont permis de m'armer, de se renforcer et de poursuivre toujours mes travaux avec succès. Je tiens également à souligner que la confiance qu'il a mise en moi a été un moteur à ma réussite.

Je remercie profondément tous les membres de jury

- Pr. Othman FILLALI MEKNASSI, Ecole Nationale des Sciences Appliquées de Tanger (Président)
- Pr. Fattehallah GHADI, Vice Président de l'Université Ibn Zohr-Agadir (Rapporteur)
- Pr. Mohammed BOULMALF, Université Internationale de Rabat (Rapporteur)
- Pr. Abdelali ASTITO, Faculé des Sciences de Techniques de Tanger (Rapporteur)
- Pr. Driss BENHADDOU, College of Technology, University of Housston (Examinateur)
- Pr. Mohammad AL-TURKISTANY, Umm AL-Qura University-Makkah, (Examinateur)

qui ont accepté d'évaluer, de juger mon travail et d'assister à ma soutenance.

Ma reconnaissance se tourne particulièrement vers les Professeurs : BEN AHMED Mohamed, Abderrahim GHADI, Khalid TOUIL, pour leurs conseils, leurs remarques et critiques pertinentes, qui m'ont conduit vers la bonne voie dans mes recherches.

J'exprime ma gratitude à :

- Pr. Chakir ELAMRANI, Chef du Département Génie Informatique
- Pr. Hassan ZILI, Professeur à la FST de Tanger,
- Pr. Abdelhadi FENNAN, Professeur à la FST de Tanger,
- Pr. Abdellah AZMANI, Professeur à la FST de Tanger,
- Pr. Benaissa AMAMI, Professeur à la FST de Tanger,

Pour leurs aides, soutiens et encouragements pour l'accomplissement de cette thèse.

Egalement, je remercie mes amis et co-équipiers du laboratoire, notamment Mr. Jaber ELBOUHDIDI, Mr. Mohamed GHAILAN pour les nombreuses et fructueuses et enrichissantes discussions, pour leur enthousiasme, volontés et esprit de recherche.

Il m'est agréable de remercier chaleureusement tous ceux qui, en dehors du laboratoire, m'ont accompagné et soutenu. Je pense particulièrement à mes parents, à mes frères, à ma femme et à ma sœur qui m'ont beaucoup aidé et supporté. Ces remerciements seraient incomplets sans un remerciement adressé aux membres de ma grande et petite famille. Ce travail leur appartient à tous. À toutes ces personnes, je serais éternellement reconnaissant.

Tanger, le 20 mai 2013.

"Contributions à la consommation de l'énergie dans les Réseaux de capteurs sans fil pour la sésurité, le routage et localisation."

Résumé

Les réseaux de capteurs sans fil (RCSF) sont des systèmes embarqués, autonomes, auto-configurables, auto-organisables et déployés dans diverses applications de contrôle et de sécurité. Dans leur architecture, les batteries de ces capteurs ne peuvent en aucun cas être remplacées ou chargées. Pour cela, il faut penser à réduire l'énergie consommée lors de la capture, du traitement et de la transmission de données.

Devant la diversité des problèmes qui se posent dans les RCSF, le challenge de la consommation de l'énergie est toujours abordé dans divers travaux de recherche en vue d'optimiser la consommation d'énergie et de maximiser la durée de vie du réseau. A cet effet, nous avons évoqué l'axe des technologies et standards implémentés dans ces capteurs, en vue de révéler leurs impacts sur la consommation d'énergie. Ensuite, nous avons soulevé les techniques de localisation affectant à leur tour cette énergie, notamment lors de l'utilisation de GPS (Global Positioning System), considéré comme solution gourmande en énergie. Le volet de sécurité a été abordé, vu qu'il se base sur la technique de la cryptographie et ôte pour la gestion des clefs pour assurer la communication entre les nœuds du réseau. Cette technique est connue par son traitement aggravé épuisant davantage l'énergie du capteur, devant la coexistence d'une multitude d'attaques qui visent la mort prématurée du réseau. Au niveau routage, la problématique d'énergie perdue lors de l'utilisation des mécanismes de découverte de routes, ouvre un champ très fertile, que nous avons attaqué, pour la conception d'algorithmes optimisés et protocoles de routage qui économisent mieux l'énergie de diffusion des messages RREQ (Route REQuest).

Notre but principal dans cette thèse, est de répondre à l'ensemble de ces défis en agissant sur les fonctionnalités d'un capteur, notamment celle de localisation, de sécurité, de routage ainsi que celle qui concerne la technologie adoptée pour assurer la communication. Des applications ont été envisagées pour mettre en place ces fonctionnalités en l'occurrence le transport, la santé, la domotique, l'industrie et le maritime. C'est ainsi que nous présentons des travaux qui favorisent une meilleure configuration de ces fonctionnalités, tout en octroyant plus d'intérêt à des solutions qui optimisent de plus en plus la consommation de l'énergie de la batterie des capteurs, pour leur permettre une longue longévité et de profiter pleinement de leurs avantages.

Mots-clés : Optimisation de l'énergie ; Securité ; Routage ; RCSF ; NS2.

"Contributions to Energy Optimization for Localization, Security and Routing in Wireless Sensor Networks"

Abstract

Recently, the pervasive and critical nature of embedded systems like wireless networks has grown rapidly in the world of research. This growth has nowhere exempt end-user to benefit from the contributions of these technologies in everyday life. In parallel, a lot of problems have emerged and led to the call of the scientific community and researchers to look for solutions. In their architecture, the batteries's sensors can not be replaced or charged. To this point, many works consider reducing the energy consumed during the capture, processing and transmission of data. It is in this context that our works was oriented to energy consumption in WSN (Wireless Sensor Networks) considered as a major constraint and problematic.

In fact, our contribution through this thesis discusses works bearing on energy optimization techniques in WSN, considered as an Ad-hoc network. To surpass the known challenges and constraints, we act on several sensor functions to look for an optimal configuration which economize more energy of sensor and maximize the network lifetime. In add to the energy optimization, the presented work adapts the results and solutions to numerous application like transport, health control, security and indoor areas.

To carry out our work, we began by conducting a comparative study of communications technologies functions in WSN. Being emerged on topics related to news on wireless sensor networks, we treated on the next the localization function by the use of the energy of transmission. Subsequently, we discussed the security function by a new approach based on the notion of agent. Finally and in the routing function, a new algorithm is presented to minimize the network load caused by the route discovery mechanisms RREQ (Route REQuest).

As an application, a deployment architecture, location and health monitoring of pilgrims is proposed for implementation in the areas of the Great Mosque of El Hajj.

Briefly, this work contributes advantageously to optimize and improve battery power of sensors in the context of their use or application domain that influences more this consumption.

Keywords : Energy Optimization ; Security ; Routing ; Sensor Networks ; NS2.

Table des matières

Liste des figures

ACRONYMES

AES	Advanced Encryption Standard
AOA	Angle Of Arrival
ADV	Advertisement
AODV	Ad Hoc On demand Distance Vector
BSS	Base Station Service
CBR	Constant Bit Rate
CMOS	Complementary Metal Oxide Semiconductor
CPEQ	Cluster based Protocol Even-driven and Query
CSMA-CA	Carrier Sense Multiple Access-Collision Avoidance
DSR	Dynamic Source Routing
ESS	Extension Station Service
FCC	Federal Communication Commission
FTP	File Transfer Protocol
GFSK	Gaussian Frequency-Shift Keying
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial Scientific Medical
MEE	Mean End to End
NOAH	NO Ad Hoc
NS2	Network Simulator 2
QOS	Quality Of Service
DRREQ	Dichotomic Route Request
RREQ	Route Request
QPSK	Quadrature Phase-Shift Keying
GPS	Global Positioning System
TDOA	Time Difference Of Arrival
TFS	Temps de Fin de Simulation
UWB	Ultra Wide Bande
WiMax	Worldwide interoperability for Microwave access
WLAN	Wirless Local Area network
WMAN	Wirless Metropolitan Area network
WMSN	Wireless Multimedia Sensor Network
WPAN	Wirless Personnel Area network
WSN	Wireless Sensor Network
WWAN	Wirless Wide Area network

INTRODUCTION AND ORGANIZATION

1

ABSTRACT

"This part of thesis presents an introduction to the main objectives to approach the reader to the goal and the basis of the realized works. It describes also a global presentation of this manuscript. In the same area, several works are done and achieved. To position our works, related works are presented here to have a global idea and identify research directions in the WSN versus energy challenge."

1.1 General Introduction

In order to surpass wired connections in the world of communication, the subject of wireless networks becomes increasingly a major concern of researchers in the world. Despite the limitations observed, these networks are in fast development with moderately increased speed. In telecommunications, before the advent of GSM, the fixed phone reigned for a long time and continues to exist today. In the same way networks and standards, like Wi-Fi, WiMax, ZigBee and UWB, will continue their development over next years, with coexistence of infrastructure-based wired in a hybrid architecture that can't be overcome.

With the development of tools based on their physical architecture on the radio frequency modules, communication, monitoring and control through wireless technology are becoming increasingly demanded in various applications. On the same way, the wireless sensor networks (WSN) have also evolved allowing the communication of information collaboratively by introducing both concepts of embedded systems, telecommunications and computer science. Considered as a specific Ad hoc networks, WSN these inherit several characteristics of these networks while offering a number of constraints and problems, classified in the heading of challenges that researchers deploy more efforts to control them. Generally, the network operates for long periods of time with wireless nodes, so the available energy resources limit their overall operation. The life time of a sensor network in which most nodes are battery-powered or non-rechargeable is essentially influenced by the used communication. Due to this, and for minimizing energy consumption, most of sensors, including the radio module, are likely being turned off most of the time.

These constraints can be increased when achieving large data like multimedia information compared to data transmitted by traditional sensors. Other challenges are present in this kind of application domain like security of transmission, localization of transmitter or receiver of data in network and the energy as a major issue and defy which affect of the listed challenges.

Computing and distributing key management for security, localizing sensors, the capture of multimedia information like audio and video are all applications of wireless sensor networks which require to meet the challenges of reliability and energy constraints. This is why we need today to develop researches on communication in WSN taking into consideration relevant cited constraints which present an important area of researches.

In most areas of research related to wireless sensor networks, the energy challenge is omnipresent, especially when using the key management for security, in the localization process when looking for a particular sensor. We note also the contribution of communication standards that mention the consumption of energy ration as inevitable problem. Indeed In this field we consider a platform-based agent targeting the application layer of the architecture of the sensor. Routing is an important key to solve and optimize the consumption while acting on the mechanisms of communication, route discovery and response.

To have an optimal configuration of sensor functionalities, we focus on energy consumption on many axes like Technology of communication, localization, security and routing protocols. At first, we compare, in term of QoS (Quality of Service) showing the role of UWB in energy consumption compared to the ZigBee. At the second work based on localization function, a localization technique is discussed to position mobile objects in the field of transportation for energy optimization. Thirdly, in the security, distribution and calculation of key application consume more energy. In this field, we propose a function based on an agent platform targeting the application layer of the architecture of the sensor without using the key method known in this domain for energy economization. After, regarding the routing function, we develop a routing protocol Dicho_AODV under the NS2 tool based on dichotomic approach used in discovery mechanism to energy economization, avoiding network saturation. Finally, we propose architecture, as an application of a hybrid localization technique and using BSN (Body Sensor Networks) for health control and localization of pilgrims in the hall grand mosque in Mecca.

The chapters of the present thesis are organized like below : The first chapter listed a problematic of research observed for the WSN domains, then it present a related works from the literature and community of researchers in order to give an idea to the lecturer about the axes, challenges and proposed solutions. The last section of this chapter outlines the methodology of research adopted and describes the organization of the thesis.

The second chapter, emerge the lecturer in the state of art of the wireless sensor networks by listing the approaches and thematic areas in conjunction with sensor networks and preparation of the work carried out the main axis of this thesis. In this sense, the literature is so rich. Although this literature traits more topics of WSN, but also list the famous challenges which attract the most research community.

Third chapter is focused on the realized works in term of the presented functionalities. The architecture of this chapter adopted an American model organizing it on sections. Every section lists a detail of research paper. The five sections give details of the results of published work in security, localization, energy towards standards, routing, and energy. The final chapter concludes the work of this thesis and states a perspective that may be a result of this work. In this context, a study was conducted in the thematic areas of the thesis targeting an application health monitoring and localization of pilgrims in the great mosque of el hajj.

1.2 Problematic of Research Focus of Thesis

1.2.1 Problematic of research

Work in the subject of sensor networks imposes confrontations to several challenges, including problems related to wireless communication, security, network density, environmental factors, transmission channel, size sensor, energy transmission and reception where is impossible to charge the battery of sensors deployed in hundreds in wide fields. The literature of this field of research includes many issues that remain open to scientific research which can be cited as an indication and cannot be limited to :

Power and energy constraints :

Power consumption is often an issue that needs to be taken into account as a design constraint. The sensor node lifetime have a strong dependency to the battery life. Generally, the wireless sensor node has a limited power source ($< 500mA, 1.2V$). Battery operation for sensors used in commercial applications is typically based on two AA alkaline cells or one Li-AA cell. Due to this, power management and power conservation are critical functions for sensor networks, and one needs to design power-aware acting on several levels of node architecture. The function of a sensor node in a sensor field is to detect events, perform local data processing, and transmit raw and/or processed data. Power consumption can therefore be allocated to three functional domains : sensing, communication, and data processing, each of which requires optimization.

Hardware Constraint :

In the architecture of a sensor node four key components are separated and four optional components. The principal components consist of a power unit (batteries), a sensing unit (sensors and converters), a processing unit (processor and memory), and a transceiver unit. At most cases, sensor network applications uses ad hoc networking techniques; although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited to the unique features and application requirements of sensor networks.

Connectivity and Topology :

In the field of WSN, deploying and managing a high number of nodes in a fairly delimited environment requires special and advanced techniques. All the nodes inside WSN should be reachable (Connectivity) while covering the maximum possible area of environment using their sensors (Coverage), even when the nodes inside the network start to fail due to energy issues or other problems. Hundreds to thousands of sensors in close proximity may be deployed in a sensor field. The density of sensors may be as high as $27nodes/m3$. Numerous problems can be listed when increasing the density which affects strongly the connectivity of sensors causing interferences, lost of data and the premature death of the network in some cases.

Standards :

Standards are now beginning to be incorporated into sensor networks. The highest degree of standardization has occurred at the lower layers. Within-building WSNs now they use ZigBee/$IEEE$802.15.4 ; WSNs that are in the open (outside buildings and over a broad geography) may find other technologies useful. In particular, $IEEE$-based wireless LAN standards have been given consideration. $IEEE$802.11, $IEEE$802.11a is an extension of 802.11 that provides up to 54$Mbps$. $IEEE$802.11b is an extension to 802.11 that provides 11-Mbps transmission. $IEEE$802.11g provides up to 54$Mbps$. Another transmission method is free-space optics operating in the 1-mm wavelength (infrared). Infrared is license-free line-of-sight technology that operates at short range (300to3000m). The new WiMax standard ($IEEE$802.16) may also be useful for metropolitan environments, as is the application of cellular third-generation technologies. Earlier we also mentioned the Smart Dust mote, which uses the visible optical spectrum to communicate.

Security :

Security is another factor that cannot be ignored in the design of WSN. Sensor nodes in WSN use power-efficient radio transceivers for their communications. Most of the existing sensor nodes operate in unlicensed frequency bands (such as the 433MHz ISM-band in Europe with a maximum capacity of 19.2$Kbps$), but some nodes follow the $IEEE$802.15.4 standard for Personal Area Networks [$IEEE$802.15.4], that has a maximum data throughput of 250$Kbps$. Regardless of the underlying technology of the transceiver, all communications are done using a wireless channel. As a result, the information flow can be easily accessed by anyone in the vicinity. All packets are then unprotected against any kind of communication attack.

Due to this several works and researches attack the security topic involving the cryptography techniques using key management system like SKC (Symmetric Key Cryptography), PKC ((Public Key Cryptography) or hash functions. Those techniques involve a massive use of processing and cause more energy. Because of this we must think seriously to reduce this consumption to avoid the premature death of sensor.

Localization :

Several WSN applications needs to localize the node who send data in term of security, but also positioning node is an important area in other applications when looking for a destination. To this nodes must compute their positions in some fixed coordinate system, it is of great importance to design efficient localization algorithms. In large range of sensor networks, node localization can assist in many techniques or in routing. The localization can be used to monitor the progress of the children by tracking their interaction with toys and also with each other. It can also be used in hospital environments to keep track of equipments, patients, doctors and nurses. For these advantages precise knowledge of node localization in wireless sensor networks is an active field of research in wireless networking. Unfortunately, for a large number of sensor nodes, straightforward solution of adding GPS to all nodes in the network is not feasible because :

- Obstacles that block the line-of-sight from GPS satellites, GPS cannot be implemented.
- Power consumption of GPS will reduce the battery life of the sensor nodes and also reduce the effective lifetime of the entire network.
- The production cost factor of GPS is an important issue especially in dense network.
- The GPS and its antenna increase the sensor node form and size.

For this purpose, a literature propose several techniques of localization based on analytical and asymptotic models based on angular, time, signal or distance approaches :AOA (Angle Of Arriva,), TDOA (Time difference Of Arrival) , RSS (Received Signal Strength), DOA (Distance of Arrival)â

1.2.2 Focus of Thesis

Traditional WSN problems discussed in the previous section are taken into account. To this, we focus our researches to the specific functions requirements such as localization, security and routing. In add, we adapt those functions to several applications like home automation, health control, logistic or security... But mainly, we focus on an optimal energy configuration inWSNs. We conceive the main research question as follows : Which functionaities ?, for which applications ? to guranty an optimal configuration for optimization of energy consumption in wireless sensor networks.

In context of the problematic listed, we therefore focused our present work on the aspect of energy optimization considered as major challenge in the WSN. As mentioned in figure I-1, the domain adopted (Lifetime optimization, Security, Localization and Routing) attracts the community of researchers. Indeed, observing this, we decide to work on this axe treating the localization, the security and routing protocol in order to surpass the energy problematic and find or present a solution to those challenges.

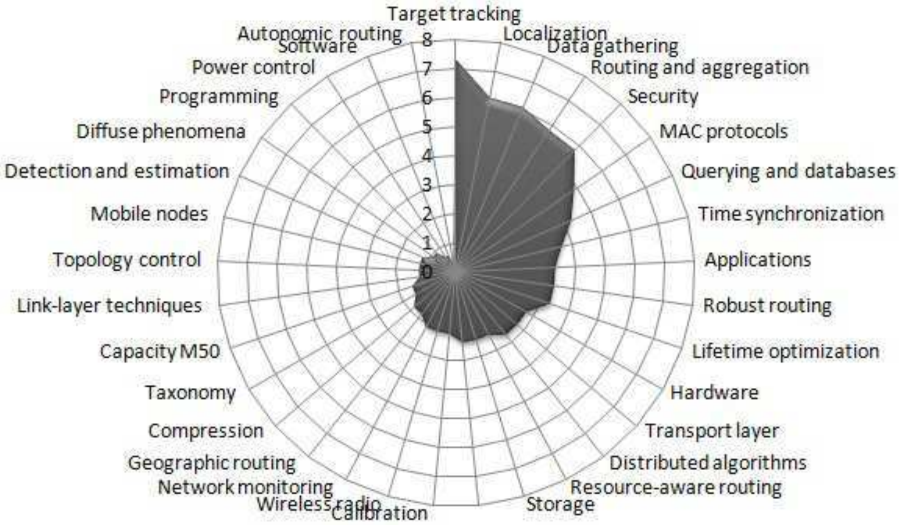


Figure 1.1 – *Classification of topic interest in WSN as number of article publication*

Involved in the communication in WSN, especially in physical layer, we act on several functionalities of sensors in order to conduct our works to hybrid and optimal configuration which consume less energy. For the first function, we study the effect of standards in the energy consumption, taking as application the transmission of multimedia data using the WMSN (Wireless Multimedia Sensor Networks) which consume more energy when achieving a heavy data using more compression technique, hence more energy consumption.

In the second functionality, the security that uses the key management approach in another focus in this thesis, considering the energy needed to compute keys and to establish communication with a negotiation process and also when a tired entity of authentication is inline. In fact, this solution consumes more energy and must be challenged to economize this energy and maximize the lifetime of sensor networks.

The localization function is another concern which not only locates a node in network but also to know who sent the data to not confuse it to the malicious one relating this field to the security. Thinking to this, a novel technique which affects faintly the battery level is a welcome for the community of researchers.

The routing function is present, especially when the mechanism of routing is truly a consistent solution for energy economization by acting algorithm optimization. Competitive works are presented in the literature trying to add a value to routing. In spite of this, this axe still open and present one field of our view to discover more optimal routing protocol from the real world and from the mathematical or analytical models.

To position the present work, the next subsection calls some related works, in the field of energy optimization, in different drift of WSN. It lists the effect of the major functionalities on the energy consumption and gives a general idea on the energy issue.

1.2.3 Related Works

Wireless Sensor Networks are becoming an essential part of our lives. Many works are focusing their researches on energy consumption like a challenge. Because of this, they work on several issues which develops many solutions to economize more energy in WSN communications.

Energy vs. Mac Layer

In [1] authors based their work on MAC layer by proposing new protocol which consists of two sub protocols : Classifier MAC (C-MAC) and Channel Access MAC (CA-MAC). C-MAC is responsible of classifying gathered data at sensor nodes based on its importance. The CA-MAC is an energy conserving medium access mechanism which uses a hybrid scheduling technique. CA-MAC saves energy by differentiating between control and data messages. Data messages are assigned scheduled slots with no contention, whereas short periodic control messages are assigned random access slots.

In [2], Chih-Yung & al. proposes efficient node placement, topology control, and MAC scheduling protocols to prolong the sensor network lifetime, balance the power consumption of sensor nodes, and avoid collision.

Energy vs Network Lifetime

In [3], Xianghui & all, propose a dynamic energy management strategy for sensors in order to optimize energy and prolonging the lifetime of WSN. The basic idea is to shut down all sensors' power when not needed and wake them up when necessary. The strategy adopted save energy of nodes, and extends the life time of nodes from one month to three month.

Cunqing Hua & al in [4]. present the technique of data-aggregation for maximum lifetime routing in wireless sensor networks. The authors optimize jointly routing and data aggregation variables. They study a comparison of DA-MLR (Data Aggregation Maximum Lifetime Routing), MEGA (Minimum Energy Gathering Algorithm) and (MER) the Minimum Energy Routing algorithms in terme of data aggregation rate and the network lifetime.

Do Van Giang & al. in [5] propose a routing algorithm for minimizing the total energy consumption and ensuring fairness of energy consumption between nodes. The authors formulate this as a nonlinear programming problem and use a sub-gradient algorithm to solve the problem. The authors formulate this problem using property of convex function to perform with good fairness index and consequently improve the lifetime of the network.

Energy vs Routing

Routing is one of the important solutions to the problem of energy efficient in wireless sensor networks. Since sensor nodes are highly energy constrained, it is essential to choose the most energy efficient routes for transferring data from the source nodes to the sink nodes.

Ali & al in [6], discuss all important concepts in WSN architecture and the impact factors that effect in performance directly or indirectly, and then they focus to power management to find best design. Their works propose a power usage model with considering clustering and routing in wireless sensor networks for the transfer of information from sensor nodes to base station. For improving this Energy they have to design a network architecture taking into account all impact components.

In [7], J. Kulik & al. develops the Sensor protocols for information via negotiation (SPIN) is a data-centric negotiation- based family of information dissemination protocols for WSNs. The main objective of these protocols is to efficiently disseminate observations gathered by individual sensor nodes to all the sensor nodes in the network. Simple protocols such as flooding and gossiping are commonly proposed to achieve information dissemination in WSNs. Flooding requires that each node sends a copy of the data packet to all its neighbors until the information reaches all nodes in the network. Gossiping, on the other hand, uses randomization to reduce the number of duplicate packets and requires only that a node receiving a data packet forward it to a randomly selected neighbor. The simplicity of flooding and gossiping is appealing, as both protocols use simple forwarding rules and do not require topology maintenance. The performance of these algorithms in terms of packet delay and resource utilization, however, quickly deteriorates with the size of the network and the traffic load.

In [8], Heinzelman & al. proposed a distributed data gathering protocol called LEACH (Low Energy Adaptive Clustering Hierarchy), for a sensor network which a fixed number of homogeneous nodes are distributed randomly over a region. Nodes are organized into clusters, and the cluster head nodes are chosen from among the sensor nodes. One of the most important characteristics of LEACH is node homogeneity. In order to use cluster head rotation, it is necessary that every node must be equipped with complex hardware for long range communication with the remote base station. This results in an increased hardware cost of the overall network.

In [9], Lindsey & al., propose a data gathering scheme called PEGASIS (Power-Efficient Gathering in Sensor Information Systems) for a homogeneous sensor network. In this scheme there is a single cluster head node, and this role of cluster head is rotated periodically over all the nodes as in LEACH. Both LEACH and PEGASIS are based on the data aggregation by the difference that the last protocol uses it at each hop by contract to LEACH who use one fixed packet size of an aggregation.

Energy vs. Security

In other hand, we can't elaborate the WSN domain without talking about WSNs security. Due to the limited capabilities of sensor nodes in terms of computation, communication, and energy, providing security to WSNs is challenging. The sensor networks are exposed to security attacks due to the broadcast nature of the transmission medium. in addition, WSNs are more fragile to attacks because nodes are often placed in a hostile or dangerous environment where they are not physically protected. For a large-scale sensor network, it is impractical to monitor and protect each individual sensor from physical or logical attack. Attackers may device different types of security threats to make the WSN system unstable.

The method of implementing WSNs security is adaptive and dynamic, which knows a continuous improvement. In [10], the authors present a survey of security approaches based on game theory in WSNs. According to different applications, a taxonomy is proposed, which divides current existing typical game-theoretic approaches for WSNs security into four categories : preventing Denial of Services (DoS) attacks, intrusion detection, strengthening security, and coexistence with malicious sensor nodes. The main ideas of each approach are overviewed while advantages and disadvantages of various approaches are discussed. Then, this paper overviews related work and highlights the difference from other surveys, and points out some future research areas for ensuring WSNs security based on game theory, including Base Station (BS) credibility, Intrusion Detection System (IDS) efficiency, WSNs mobility, WSNs Quality of Service (QoS), real-world applicability, energy consumption, sensor nodes learning, and expanding game theory applications and different games. Thus, a global view of WSNs security approaches based on game theory is provided. To our best knowledge of knowing, it is the unique work focusing on game theory in WSNs security.

In [11], the authors identify the threats and vulnerabilities to WSNs and summarize the defense methods based on the network protocol layer's analysis. They also proposed security suggestions based on Cryptography and Key management, securing routing, data fusion and aggregation mechanisms. But they don't mention to the energy consumption as a major concern that can be affected by the security process in wireless communication.

The authors in [12] survey the use of concepts of game theory to solve the problems of energy efficiency, security, and detection and tracking in WSNs. They present a cooperative sensor networks with problem formulations based on the nature of interaction between nodes in wireless sensor networks. In fact, the idea is to apply models from theories that model the behavior of sensor networks from a rational point of view. The authors solicit the use of distributed algorithms to achieve increase in network lifetime and reliable network operation in order to increase interaction between nodes.

Energy vs Localization

In WSN, like many attractive applications such as security, routing and tracking, knowing the accurate locations of sensor nodes take an important area in the researches. The Localization that means the position coordinates of sensor node in WSN can add significant meaning to information which is collected by sensors.

In [13] Amitangshu Pal reviews different approaches of node localization discovery in wireless sensor networks. The overview from the literature for the improvement of localization in wireless sensor networks is also presented to mention to the importance to localization topic.

In [14] Guoqiang Mao & al. list an overview of the measurement techniques in sensor network localization and the one-hop localization algorithms based on these measurements. They also present multi-hop connectivity-based and distance-based localization algorithms. A discussion of the localization as an open research problems in the area of distance-based sensor network.

In [15], Larios & al. present a localization system LIS (Localization based on an intelligent distributed fuzzy system to locate and track of wild animals in natural parks. The LIS system is a fuzzy algorithm for localization proposed to reduce the energy consumption. LIS combines a fuzzy system to estimate the distance between the transmitter and the receiver from RSSI measures, and a distributed algorithm executed in receiver anchor nodes in order to determine the relative positions to them and filter useless information, and a centralized algorithm to derive the most likely location running at the Base Station.

In [16] Xing-Hong & al. proposed node localization scheme noted virtual beacons-energy ratios localization (VB-ERL) and based on the Gauss-Markov mobility model. In this scheme, all nodes are static and the unique mobile node move in the surveillant field and periodically broadcast the information packets. Each static unknown node receives the virtual beacons and energy in its sensing range, and estimates its location by finding the intersection of a set of hyper-spheres.

The literature is rich on the topic of energy consumption, but still a relevant area presenting several challenges. Because of this, researches still acting on developing new propositions and solutions. In this context, the next section lists our main contributions and the methodology adopted to achieve this work.

ABSTRACT

"In the next section, a realized works and the different functionalities are summarized in this section. A working methodology, during the preparation of this thesis, is mentioned."

1.3 Main Contributions & Working Methodology

1.3.1 Main Contributions

In this thesis, we survey the important functions affecting energy consumption on the coverage of WSN, which offer new observations and interesting dimensions and point of view, and may serve as good guidelines for efficient sensor network design and producing an optimal configuration of functions which minimize the energy consumption of sensors and in fact he life time of sensor network. The main contributions of our research are described on figure 1-2 and listed as follows :

- In the first function, we are acting on the physical layer, and work on the study performance of the standards of communication in WSN by giving a comparison, in term of QoS, between the UWB and ZigBee. The comparison treats the relevant metrics End to End Delay, Packet Delivery Ratio and Energy by several simulations and scenarios under the NS2 Simulator. The results resumes to convenience of the UWB to the WSN consuming less energy in good time dissemination. This work, as it was, a start point to the thesis to emerge in the WSN domain.
- Giving to the localization an important area in WSN, the energy consumption is also affected by this functionality. In this context, and after a survey on the localization technique used till now, we propose a new technique of localization for the transport domain and based on the energy of the transmission far to the use of the GSP module, or any asymptotic technique like AOA, TDOA, RSS or TDOA. Several Simulations are done with the comparison with the TDOA technique and the NS2 measurements giving the real distance and the calculation of TDOA formula and compared to the analytical proposition base on the Euclidian distance and the energy consumed. The results shows that the presented method outperform well by giving more precisions with small angle of directional antenna.
- In the third work, we propose a security function based on agent approach, in order to surpass the key management technique. The goal here is to optimize the energy consumption of computing keys. This work attracted the application level operating on the mote (sensor) operating system (TinyOs).
- Routing function is another concern of our work, in this field the algorithm optimization is one of the great solution to the energy economization. We present a novel protocol based on dichotomic approach to reduce the route discovery mechanism compared to the AODV protocol. Under the NS2 simulator, acting on the protocol implementation is one of complex programming challenge.
- In the last work, we discuss and propose an application of some results of research in a system dedicated for control and monitoring of pilgrims. Indeed, this allows, using a BSN (Body Sensor Network) as a particular application of wireless sensor network, for the localization of lost pilgrims and control, in real- time, the health status of those who fall into critical situation with diseases that could threaten their health and life. The solution, present a model for an area, and

which can be duplicated for the full area of El hajj. It also facilitates the intervention and localization, in real time, of pilgrims who are away from their camps and to save their life.

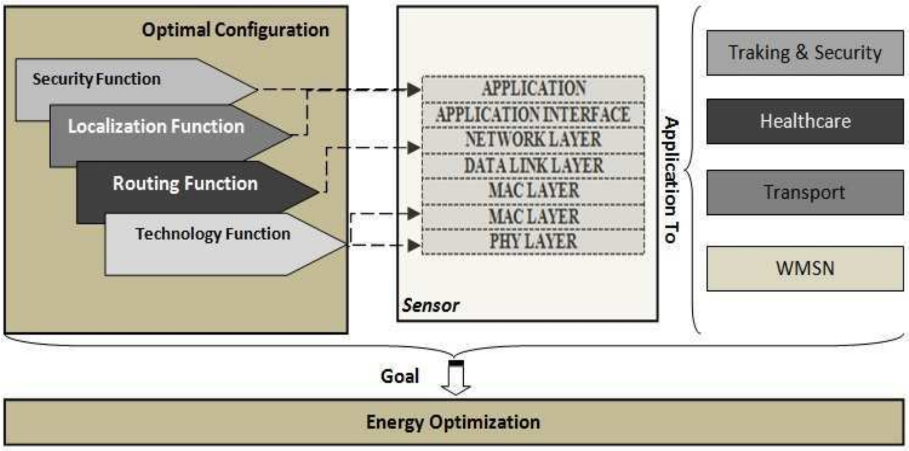


FIGURE 1.2 – *Description of the thesis's focus*

1.3.2 Working Methodology

To achieve results in original quality, we are adopting a methodology (figure 1-3) that allows a successful work and arrive to submit works on new and relevant axes of research. To do this, we started by looking for more documentation in order to clarify and identify the main scheme that lead to solving the problematic related to our line of research. A study on surveys on sensor networks allowed us to formulate gradually the main problematic. A global vision of the supervisor was very beneficial to focus on the topic, produce papers and contribute in several events. In fact, participation in national and international conferences helped us to remain more related changes and news of our subject.

Related to the main subject of the thesis, and after several researches, we try to propose a hybrid or optional solution composed from the relevant functionalities (Security, Localization, Routing and Technology). We referred to an optimal configuration which economizes more energy of sensor and network life.

Practically, the adoption of an open source simulation tools (NS2) allowed us to better control and knows its architecture and its use in the simulation of wireless sensor networks and use it in all performed works. NS2 software simulator is an Ad hoc networks massively used in

the domain of research and especially when adopt an energy model in add to its opening to the community research. This tool allows the implementation of several protocols in security, localization, in energy optimization and more.

Before turning in this report, several studies have been submitted and validated by scientific comities and have been published in many indexed and international journals. Meanwhile, collaborations are being validated to cooperate and to work on common research center with the university Umm Alkoura of Saudi Arabia, will give advanced in the practical application of this work.

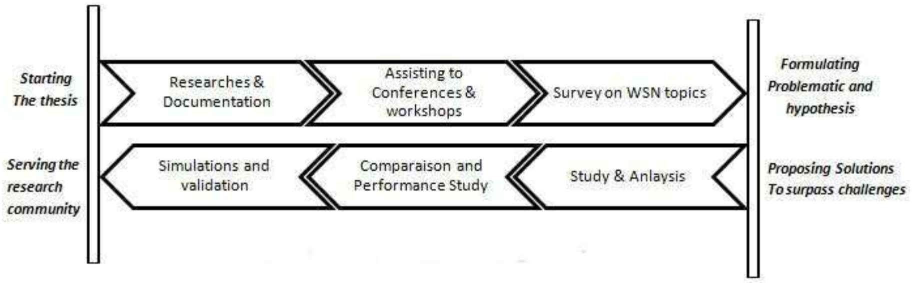

Starting
The thesis
Researches & Documentation
Assisting to Conferences & workshops
Survey on WSN topics
Formulating Problematic and hypothesis
Serving the research community
Simulations and validation
Comparaison and Performance Study
Study & Anlaysis
Proposing Solutions To surpass challenges

Figure 1.3 – *Global vision to working methodology*

The next section gives a list of the productions dons in term of published articles in international journals and papers communicated in internationals conferences and workshops.

ABSTRACT

"The section below lists the main contributions in term of publications in international journals and the communications in conferences and workshops"

1.4 Personnel Publications & Communications

1.4.1 PUBLICATIONS IN INTERNATIONALS JOURNALS

(1). A.A.BOUDHIR, BOUHORMA MOHAMED, BEN AHMED MOHAMED "New Technique of Wireless Sensor Networks Localization based on Energy Consumption", International Journal of Computer Applications (IJCA) November Issue (Vol.12 N.7), 2010, ISSN : 0975-8887

(2). A.A.BOUDHIR, M.BOUHORMA, M.BEN AHMED "Multi-Agents Platform for Security in Wireless Sensor Networks", International Journal of Computer Science and Network Security October Issue, (Vol. 10 N. 10), 2010, ISSN : 1738-7906

(3). A. A. BOUDHIR, M. BOUHORMA, M. BEN AHMED, ELBRAK SAID "The UWB Solution for Multimedia Traffic in Wireless Sensor Networks", International Journal of Wireless & Mobile Networks (JWMN), October Issue, (Vol. 3, No. 5), 2011, ISSN : 0975-3834

(4). A. A. BOUDHIR, M. BOUHORMA, M. BEN AHMED, ELBRAK SAID "New Algorithm "DRREQ" Applied in AODV Route Discovery Mechanism for Energy Optimization in Mobile Ad hoc Networks", International Journal of Computer Engineering Science (IJCES), December issue, (Vol.1N.3), 2011, ISSN : 2250-3439

(5). A.A.BOUDHIR, M.BOUHORMA, M.BEN AHMED, ELBRAK SAID "A Real Time Health Control and Localization of Pilgrims in El Hajj : BSN Application", Journal of Theoretical and Applied Information Technology (JATIT) Accepted for Publication in April 2013, ISSN : 1992-8645

(6). A.A.BOUDHIR, BOUHORMA MOHAMED, BEN AHMED MOHAMED "Energy Optimization Approaches In Wireless Sensor Networks : A Survey", International Journal of Networks and Systems (IJNS) November Issue (Vol.1 N.1), 2012, ISSN : 2319-5975.

1.4.2 COMMUNICATIONS IN CONFERENCES

(1). BOUHORMA, M. ; BOUDHIR, A. ; BEN AHMED, M. ; EL BRAK, S. "New route request mechanism for energy optimization in mobile ad hoc networks", Telecommunications Forum (TELFOR), 2011 19th, November, IEEEXPLORE, 10.1109/TELFOR.2011.6143533, 2011.

(2). BOUDHIR, M. BOUHORMA, , M. BEN AHMED "Wireless Sensor Networks and Communication Protocols for Transport Localization", International Scientific Congress Of Engineering-CCII-2010 3- 5 Mars 2010.

(3). A. BOUDHIR, M. BOUHORMA, , M. BEN AHMED "Quality of Service and Energy Consumption in Uwb and ZigBee Standards Applied To Wireless Multimedia Sensor Networks", Workshop on Next Generation

Mobile Networks -WNGMN'09- November 14-15, 2009.

(4). A. BOUDHIR, M. BOUHORMA, , M. BEN AHMED "Multi-Agents Platform for Security in Wireless Sensor Networks", Journées Franco-Maghrebine Micro Ondes et Applications 2011 (JFMMA2011).

(5). A. BOUDHIR, M. BOUHORMA, , M. BEN AHMED "Energy Based Localization for Wireless Sensor Networks Applied to Transport", Journées Franco-Maghrebine Micro Ondes et Applications 2011 (JFMMA2011).

(6). A.A.BOUDHIR, M.BOUHORMA, M.BEN AHMED,S. ELBRAK "A Survey on Energy Optimization in Wireless Sensor Networks", 2nd Forum des Jeunes Chercheurs (IIémeFJC'2011).

(7). A.A.BOUDHIR, M. BOUHORMA, M. BEN AHMED and ELBRAK SAID "New Algorithm "DRREQ" Applied in AODV Route Discovery Mechanism for Energy Optimization in Mobile Ad hoc Networks" Third Edition of ICMCS 2012 Tangier.

(8). A.A.BOUDHIR, M.BOUHORMA, M.BEN AHMED "A Real Time Health Control and Localization of Pilgrims In El Hajj : BSN Application", Accepted for oral communication in ICCAT2013, 20-22 January 2013 in Tunisia.

1.5 Conclusion

The WSN domain is a huge axe of research which can't be limited due to the diversity of challenges. To this, we are focused on an interesting topic considered as a major challenge related to the life a network sensor. In this chapter we presented a general view on the thesis by introducing the problematic of energy consumption and their related axes. We also mentioned to focal points of our work and listing a brief to all contributions and productions. To achieve this works, a global vision to the methodology adopted was presented.

The following chapter content four sections introducing a survey on relevant topics like :

- WSN,
- QoS and Routing,
- Wireless communication technologies,
- Security.

2

GENERAL SURVEY

ABSTRACT

"The section below gives a survey on the WSN considered as the main topic of the thesis. It lists the pillars of this axis and the principal basics of the literature."

2.1 Wireless Sensor Networks : A Survey

2.1.1 INTRODUCTION

The technology for sensing now has the potential for significant advances, not only in science and engineering, but equally important, on a broad range of applications relating to critical infrastructure protection and security, health care, the environment, energy, food safety, production processing, quality of life, and the economy. In addition to reducing costs and increasing efficiencies for industries and businesses, wireless sensor networking is expected to bring consumers a new generation of conveniences, including, but not limited to, remote controlled heating and lighting, medical monitoring, automated grocery checkout, personal health diagnosis, automated automobile checkups, and child care.

A sensor network is a special case of Ad hoc networks, consisting of nodes called "motes" and that stands for an Ad hoc network with their miniature size, by their characteristic unidirectional and their objectives are targeted advance compared to that of a generic Ad hoc network.

This new type of network presents a great improvement compared to conventional sensors that are typically deployed in two ways :

- The sensors are positioned away from the monitored phenomenon, in this case of devices using complex approaches are needed to distinguish the data captured environmental noise.
- Several sensors are deployed around the field monitoring. At this point, the position sensors and communications topology must be carefully designed in advance. These sensors transmit data regularly to the central node where treatments are performed and the data is merged.

In order to approach this type of network architecture and operation of these sensors, its design constraints and its applications will be mentioned in this chapter.

2.1.2 CLASSICAL WIRELESS SENSOR NETWORKS

Recent advances in wireless technology and electronics have enabled the development of tiny low cost sensors with low energy (low-cost solution and low-power). These sensors have three functions : [17]

- Capturing data (such as sound, vibration, light, etc) ;
- Calculate information using these values ââcollected ;
- The communication through a network of sensors.

A sensor network is composed of a number of often very important nodes that are either placed in a specific location or scattered randomly (often deployed by air using helicopters or airplanes). This random dispersal of sensors requires that the protocol for sensor networks has self-organizing algorithms. To withstand the deployment, these sensors must be very strong and more, they must also be able to survive in extreme conditions dictated by their operating environment (eg water or fire). In addition to environmental constraints, a major constraint is the battery saving. Indeed, a sensor network cannot survive if the loss of nodes is too large as this causes loss of communication due to too great a distance between the sensors. So it is very important that the batteries last as long as possible because in most applications they are randomly placed (impossible to return to change the batteries). This use linked to the autonomy of the sensors (one year maximum for current technology) involves a significant parameter which is the price. No application would be profitable if the ratio of hours of use / price was too high. It was therefore necessary to combine technology and low cost.

Sensor networks can be programmed to a number of purposes, such as control of intrusion, the calculation of temperatures, the calculation of climate change, monitoring of animal movements (with GPS), patient monitoring, etc.

Architecture of a Wireless Sensor Network

In a WSN, sensor nodes are organized into fields "sensor fields" (figure $2-1$). Each of these nodes has the ability to collect data and transfer them to the gateway node (called "sink" in English or sink) via a multihop architecture [17]. Well then transmits this data via the Internet or satellite to the central computer "Task Manager" to analyze and make these decisions.

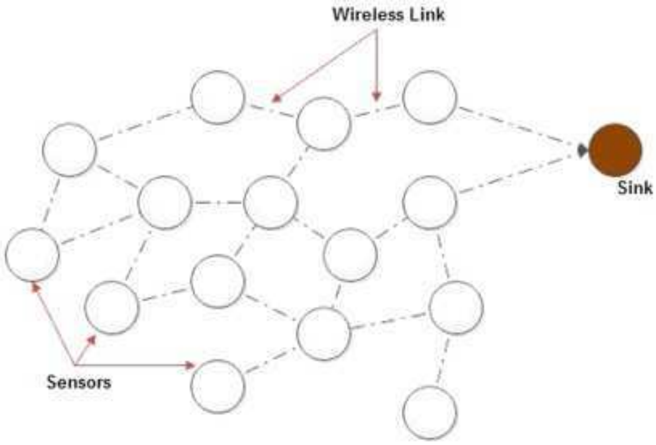


FIGURE 2.1 – *WSN field*

Anatomy of a sensor node

A sensor node, or mote, is mainly composed of a processor, memory, a radio transmitter / receiver, an embedded system with the sensor unit and a battery [17]and [18]. (figure $2-2$).

Cycle of operation and energy sensor

The node can go to sleep (sleep mode) or just listen traffic. The transmission unit is the unit that consumes the most energy by supplying the units comprising a sensor. (figure $2-3$)

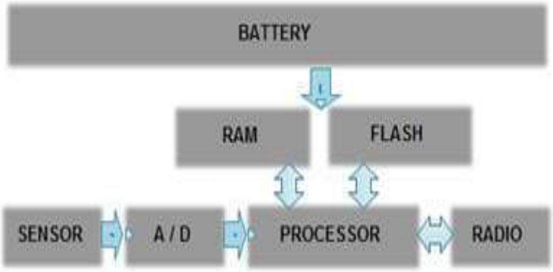


FIGURE 2.2 – *Sensor Anatomy*

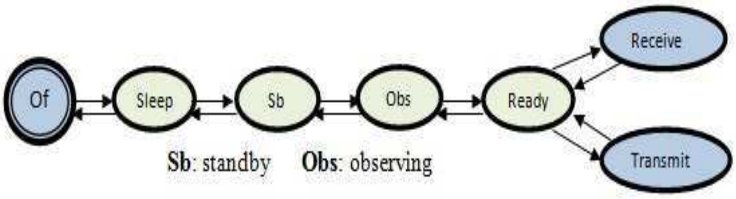


FIGURE 2.3 – *Sensor Operation Cycle*

For a bit and distance between two nodes, the Radio module (figure $2-4$) of a node consumes energy when transmitting energy $T_x(l,d)$ and $R_x(s)$ upon receipt :

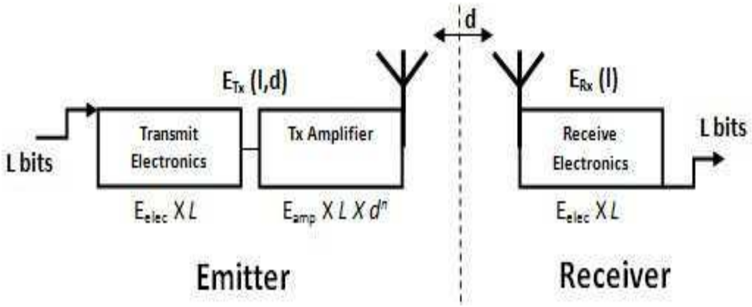


FIGURE 2.4 – *Energy Consumption of Radio Model*

Radio transmission Consumption ξ_{Tx} [19] : The energy consumed during the transmission of bits between two nodes (transmitter and receiver) is expressed by :

$$\xi_{Tx}(l,d) = \xi_{Tx} - \xi_{elec}(l) + \xi_{Tx} - \xi_{amp}(l,d)$$

$$\xi_{Tx}(l,d) = \xi_{elec} * l + \xi_{amp} * l * d^2$$

Radio reception Consumption ξ_{Rx} [20] :

$$\xi_{Rx}(l) = \xi_{elec} * l$$

with :

$$\begin{cases} \xi_{elec} : \text{energy transmission / receiving of electronic device;} \\ l : \text{size of a message;} \\ d : \text{distance between the transmitter and receiver;} \\ amp : \text{amplification factor.} \end{cases}$$

There are several models available on the market, Among the most famous :

– "mote" MICAx ;

– TelosBe Crossbow (http ://www.xbow.com).

Example :

The following figure (figure $2 - 5$) shows the components of a sensor node TmoteSky :

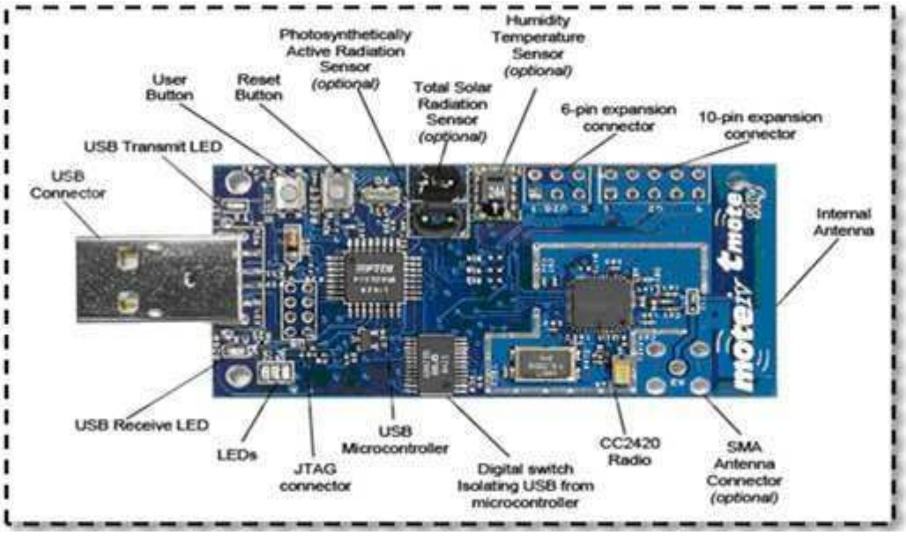

Photosynthetically Active Radiation Sensor (optional)
Humidity Temperature Sensor (optional)
User Button
Reset Button
Total Solar Radiation Sensor (optional)
6-pin expansion connector
10-pin expansion connector
USB Transmit LED
USB Connector
Internal Antenna
tmote sky
USB Receive LED
LEDs
JTAG connector
USB Microcontroller
Digital switch Isolating USB from microcontroller
CC2420 Radio
SMA Antenna Connector (optional)

Figure 2.5 – *Sensor Face of "TmoteSky"*

Constraints Design of WSN

The main factors influencing the architecture and constraints of sensor networks can be summarized as follows :

Fault Tolerance : Some nodes may generate errors or stop working because of a lack of energy, a physical or interference. These problems do not affect the rest of the network ; it is the principle of fault tolerance. Fault tolerance is the ability to maintain network functionality without interruptions due to a fault occurring on one or more sensors.

Scale : The number of nodes deployed for a project may reach one million. Such a large number of nodes generates a lot of transfers inter nodal and requires that the well "sink" is equipped with lots of memory to store the information received.

Production costs : Often, sensor networks are composed of a very large number of nodes. The price of a node is critical in order to compete with a network of traditional surveillance. Currently a node does not often costs much more than $1. For comparison, a Bluetooth node, already known to be a low-cost system, costs about $10.

The environment : The sensors are often deployed en masse in places such as battlefields beyond enemy lines, inside large machines, the bottom of an ocean, fields biologically or chemically contaminated. Therefore, they must operate unattended in remote geographic areas.

Network topology : The deployment of a large number of nodes requires maintenance of the topology. This maintenance consists of three phases : Deployment, Post-deployment, and Redeployment of additional nodes.

Material constraints : The main constraint is the physical size of the sensor. Other constraints are that energy consumption must be reduced so that the network will survive as long as possible, it adapts to different environments (extreme heat, water, etc.), it is very durable and autonomous since it is often deployed in hostile environments. [17].

The media transmission : In a sensor network, nodes are connected by a wireless architecture. To allow operations on these networks worldwide, the transmission medium must be normalized. We mostly use the infrared (which is license-free, robust to interference, and inexpensive), Bluetooth and ZigBee radio communications.

Energy consumption : A sensor, because of its size, is limited in energy ($< 1.2V$). In most cases the battery replacement is impossible. This means that the lifetime of a sensor depends greatly on the life of the battery. In a sensor network (multihop) each node collects data and transmits values. The failure of some nodes requires a change in network topology and a re-routing of packets. All these operations are energy intensive, it is for this reason that current research focuses primarily on ways to reduce consumption.

Applications of Wireless Sensor Networks

The WSN can have many applications. Among them, we quote : [18]

- Discovery of natural disasters can create standalone network nodes by dispersing in nature. Of sensors can report events such as forest fires, storms or floods. This allows a much more rapid and effective relief.
- Intrusion detection : By placing at various strategic points, sensors, and can prevent burglaries or passages of game on a railway track (for example) without having to resort to expensive video surveillance devices.
- Business Applications : One could imagine having to store food that requires some moisture and a certain temperature (max or min). In these applications, the network must be able to collect various information and alert in real time if critical thresholds are exceeded.
- Pollution control : sensors could disperse over an industrial site to detect and control leaks of gas or chemicals. These applications would provide warnings in record time and to monitor the disaster.
- Medical Surveillance : By implanting under the skin of mini video sensors, one can receive real-time images of a body part without any surgery for about 24 hours. We can monitor the progress of a disease or reconstruction of a muscle.
- Control structures : Insert additional dams on the walls of sensors to calculate in real time pressure. It is therefore possible to regulate the

water level if the limits are reached. One can also imagine include sensors between the sandbags forming a makeshift dam. Early detection of water infiltration can be used to reinforce the dam accordingly. This technique can also be used for other constructions such as bridges, railways, mountain roads, buildings and other structures.

2.1.3 WIRELESS MULTIMEDIA SENSOR NETWORKS

The technology boom in electronics contributed to the availability of equipment miniaturized and low cost such as CMOS cameras and microphones which helped further the development of sensor networks wireless multimedia (WMSN), devices that are able to recover the ubiquitous multimedia content such as streaming audio and video, still images, and data from environmental sensors. Sensor networks Wireless multimedia will not only strengthen the networks of sensors such as monitoring, home automation and environmental monitoring, but they will also enable several new applications [21] such as :

- Monitoring Networks Multimedia,
- Storage of potentially relevant
- Traffic Control Systems,
- Medical Surveillance Remote
- Environmental monitoring,
- Location Services,
- Industrial Process Control,
- Etc.

Anatomy of Multimedia Sensor Networks

The problem of designing scalable network architecture is of great importance. Rates for most networks are wireless sensor architecture based on a flat, homogeneous wherein each sensor has the same physical and can only to interact with adjacent sensors. Traditionally, research on algorithms and protocols for sensor networks has focused on adaptability, that is to say, How to design solutions whose applicability is not limited by the size before growth the network. The flat topology cannot always be agreed to handle the amount of traffic generated by multimedia applications including audio and video. Similarly, the processing power required for data processing and communications the power required to operate, may not be available on each node.

In the previous figure (Figure 2-6) [22], we present reference architecture for WMSNS, which is illustrated three sensor networks with different characteristics, deployed in different physical locations. The first cloud on the left shows a single-level network of video sensors homogeneous. A subset of sensors deployed has the highest processing capabilities and is thus referred to as the processing centers. The union of treatment centers is a distributed processing architecture. Multimedia content gathered is relayed to a wireless gateway with a multi-step path. The gateway is connected to a storage center, which is responsible for the content of multimedia storage locally for the next recovery. Clearly, more complex structures for distributed storage can be implemented when permitted by the envi-

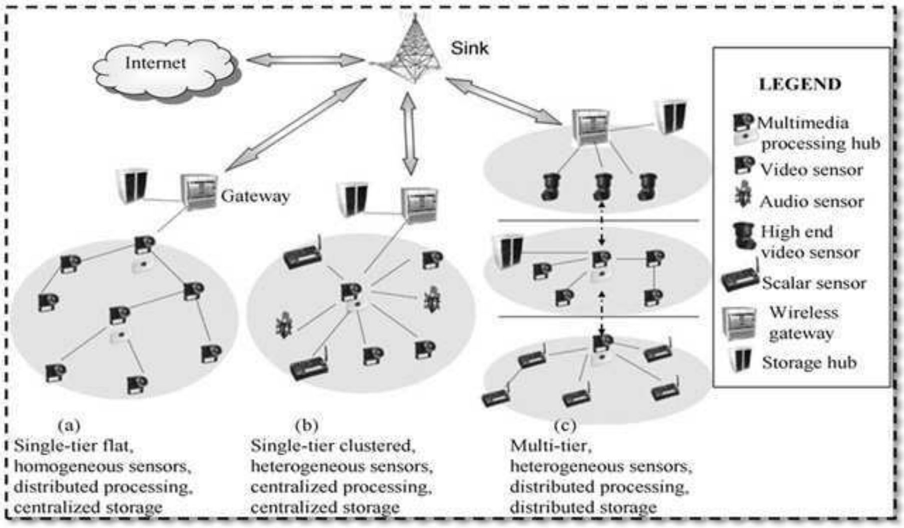

Internet
Sink
Gateway
LEGEND
Multimedia processing hub
Video sensor
Audio sensor
High end video sensor
Scalar sensor
Wireless gateway
Storage hub
(a)
Single-tier flat, homogeneous sensors, distributed processing, centralized storage
(b)
Single-tier clustered, heterogeneous sensors, centralized processing, centralized storage
(c)
Multi-tier, heterogeneous sensors, distributed processing, distributed storage

FIGURE 2.6 – *WMSN Architecture*

ronment and application needs, which can lead to energy savings since, by storing it locally, the media should not be (wireless) relayed to remote locations. [22] and [23].

Factors influencing the design of multimedia sensor networks :

Sensor networks wireless multimedia derives from a convergence of communication and calculation of signal processing and several branches of control theory and embedded computing. This interdisciplinary research will distributed heterogeneous systems and devices embedded in this direction, to interact and control the physical environment. There are several factors that mainly influence the design of a WMSN :

- Strong demand for QOS (Quality of Service)

A wide variety of applications envisaged on WMSN, [24], have different requirements. In addition to the methods of delivering digital data, sending real-time multimedia data containing triggered events and observations obtained in a short time is a critical factor. Therefore, a solid foundation is necessary in terms of hardware and support high-level algorithms to provide quality service and to consider the application specific requirements. These requirements include multiple domains and can be expressed, among others, in terms of a combination of limits on energy consumption, delay, reliability, distortion. etc.

- Application of high bandwidth

Multimedia data, particularly video, need bandwidth during transmission of magnitude higher than that supported by currently available sensors. The following table (tab1) cites the transmission rate for some sensors :(Table → figure 2-7)

- Multimedia coding techniques

Decompression of video streams requires excessive use of bandwidth for a multi-jump. (Table → figure 2-8)

Therefore, it is evident that the effectiveness of treatment techniques are lossy compression necessary for multimedia sensor networks.

- Data processing in multimedia networks

Sensor	Standard	Nomimal rate of Transmission
. Crossbow's . MICAz . TelosB . Tmote	IEEE 802 15.4	250 kbit/s

FIGURE 2.7 – *Transmission rate for some classical sensors*

Format (QCIF, $176x120$)	$21Ko$, 30 Images /s
Video Stream	plus de 5 Mbit / s

FIGURE 2.8 – *Sample of compression rate of video stream*

The data processing can execute algorithms on the raw data extracted from the environment requires new architectures for collaborative processing, distributed taking into account the resource constraint and taking into account the filtering and extraction of information wellfield. This can increase the adaptability of the system by reducing the transmission of redundant.

- The energy consumption

Energy consumption and power Supply [25] are fundamental concerns in WMSN, even more than in wireless sensor networks traditional. Made by the sensors are devices with constrained battery, while multimedia applications produce large volumes of data requiring high transmission rate and treatment at the time or energy consumption of sensor nodes is dominated by traditional communications capabilities, and is introduced by minimal effect.

2.1.4 CONCLUSION

These networks experiencing a boom thanks to the multitude of applications they offer and their inherent characteristics such as their random deployment and low cost, high mobility and also thanks to the many studies that have improved the quality of service that supply these sensors in terms of communication time, safety, quality and integrity of data to be transmitted. Indeed, research in WSN poses a number of challenges in terms of bandwidth in a position to expand it to allow the sending end of data-intensive multimedia streams namely incorporating the audio and video.

Subsequently, we will discuss the notion of QoS in WSN and using different metrics to define this notion, then quoting some protocols that address in their design and the concept of QoS algorithms.

ABSTRACT

"Being a physical and Mac layer composition, the technology integrated in the sensor is one of the most functions treated in this thesis which concern significaly the energy consumption of this devices. In this context, a general overview is scheduled to cover this element".

2.2 Wireless Communication Technologies in WSN

2.2.1 INTRODUCTION

Multiple technologies (figure 2-9) allow wireless transmission of information. Each corresponds to a different use, according to its characteristics :

- ▷ Transmission,
- ▷ Maximum flow,
- ▷ Cost of infrastructure,
- ▷ Cost of equipment connected,
- ▷ Security,
- ▷ Flexibility of installation and use,
- ▷ Autonomy and power consumption, etc.

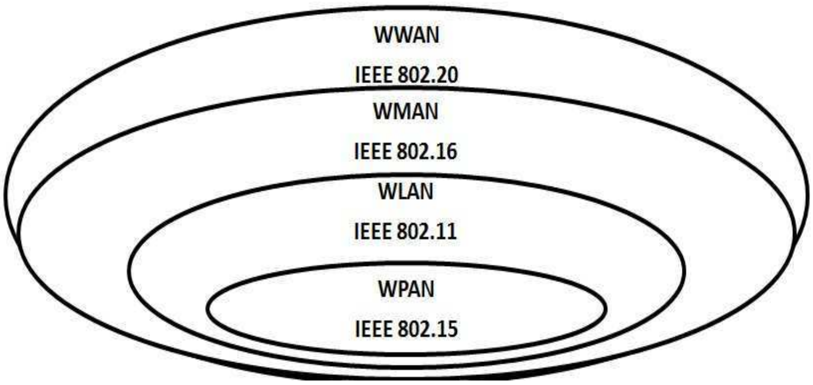


Figure 2.9 – *Technologies transmission rate*

2.2.2 STANDARD IEEE 802.15.4

The IEEE 802.15.4 standard was specifically designed for wireless sensing applications. The standard is very flexible, because it specifies data rates and multiple frequencies. And to the needs of low power consumption, the product is designed to allow the radio module is put to sleep, greatly reducing the energy consumption. Furthermore, when the node wakes up from sleep mode, the speed of synchronization on the network can be achieved. This capability allows a very low average power supply current.

- ▷ Characteristic of the IEEE 802.15.4 standard :
  - . Data rates of 250 kbps, 40 kbps and 20 kbps.
  - . Data rates of 250 kbps, 40 kbps and 20 kbps.
  - . Two addressing modes, 16-bit short and IEEE 64-bit addressing.
  - . Support for critical latency devices, such as joysticks.
  - . CSMA-CA access channel.
  - . Automatic creation of the network by the coordinator.
  - . All handshaked transfer protocol reliability.
  - . Power management to ensure low energy consumption.
  - . 16 channels in the 2.4GHz ISM band, 10 channels in the 915MHz I and one channel in the 868MHz band.

2.2.3 TECHNOLOGY ZIGBEE

A major concern addressed in wireless communications, until the near future, is the bandwidth. However, some applications, such as : home automation, security, agriculture, etc. monitoring. relax the bandwidth requirements needed for a low cost and low power consumption. Existing standards were not appropriate because of their complexity, their high cost and energy consumption induced.

In this context, the ZigBee alliance is born : it is an association of companies working together to develop a comprehensive and open standard for wireless communications with low cost and low energy consumption.

▷ ZigBee Applications :

. Home Automation : Heating, ventilation, air conditioning, security, lighting, and control objects,

. Industrial : Detection of an emergency, machine control,

. Automotive : Checking tire pressure, etc,

. Agriculture : Measurement of soil moisture, detection of situations for the use of inputs, measurement of soil salinity, etc,

. Other : Control of electronic equipment, communication between PCs and devices, etc..

▷ ZigBee Characteristics :

. The objectives of ZigBee can be summarized in the following,

. Use without geographical restrictions,

. Penetration through walls and ceilings,

. Installing automatic / semi-automatic,

. Possibility to add / remove devices,

. Cost-effective,

. Flow rate : 10kbps-115.2kbps,

. Radio range : 10-75m,

. Up to 65k nodes per network,

. Up to 100 networks co-located,

. Up to 2 years of life of standard alkaline battery.

The following figure illustrate the positioning of zigbee compared to other technologies emerged in wireless communication :

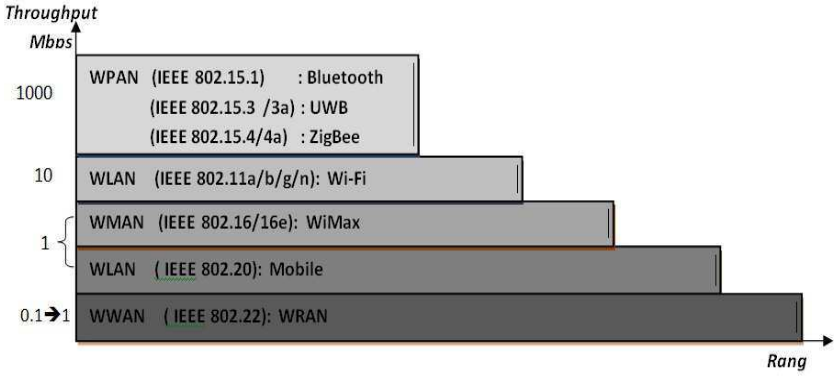


FIGURE 2.10 – *Technologies transmission rate*

▷ Architecture ZigBee / IEEE 802.15.4aa

The IEEE 802.15.4 Working : Groupâs role is the definition of lower layers : MAC and PHY. The ZigBee Alliance that brings together over 50 companies had for the role definition of the upper layers : routing application. The following figure illustrates the layered architecture of ZigBee / IEEE 802.15.4a [17].

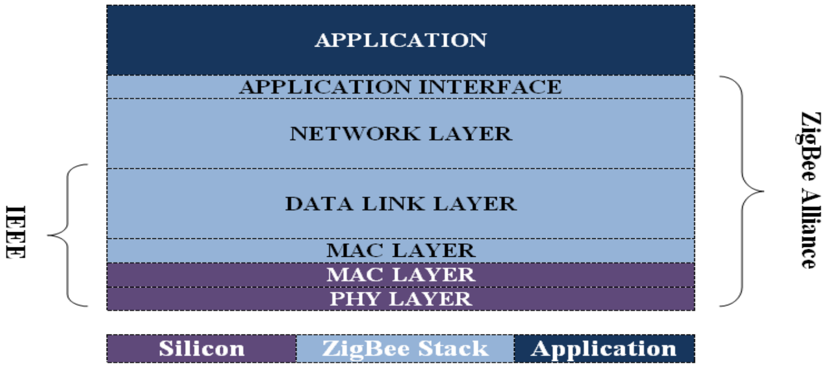


Figure 2.11 – *Protocol stack of ZigBee (IEEE 802.15.4a)*

▷ Previews MAC IEEE 802.15.4a
The IEEE 802.15.4a MAC layer :
- ○ Uses two addressing modes IEEE 64-bit 16-bit,
- ○ CSMA-CA channel access,
- ○ Uses a simple frame structure,
- ○ Allows use of the mechanism beaconing, periodic wake-up, checking the arrival of a beacon,
- ○ Saves energy through sleep between beacons, and the nodes not to route or receive data can randomly go to sleep,
- ○ Ensures reliable transmission of data,
- ○ Provides security AES-128.

. Network Beacon
- ○ Identifies the network,
- ○ Describes the structure of the super-frame,
- ○ Indicates data,
- ○ Present only when the network is active,
- ○ It is optional.

. Mechanism channel access
IEEE 802.15.4a uses CSMA / CA available in two versions depending on the configuration of the network :
- ○ If the "beaconing" is not used, IEEE 802.15.4a uses CSMA / CA without slots.
- ○ If the "beaconing" is used, IEEE 802.15.4a uses CSMA / CA with slots and super-frame structure.

2.2.4 UWB TECHNOLOGY

Ultra Wide Band technology, listed in [32] and [33], is one of the keys to these future high data rate WPAN personal networks-WBAN (Wireless Personal Area Network - Wireless Body Area Networks). It has its origins in radio and radar systems exotic two decades of the twentieth century, but has really gained momentum factor in 2002, the day the U.S. authority to regulate frequencies (FCC) took the unexpected decision to authorize the emission of UWB radio signals (of stress compliance with low transmission power).

- Characteristics of UWB signals
  - The Ultra Wide Band UWB technology involves sending energy pulses (Figure 2-12), [32] low power over a wide frequency band, to communicate wirelessly at very high speeds of up to 110 Mbps ;

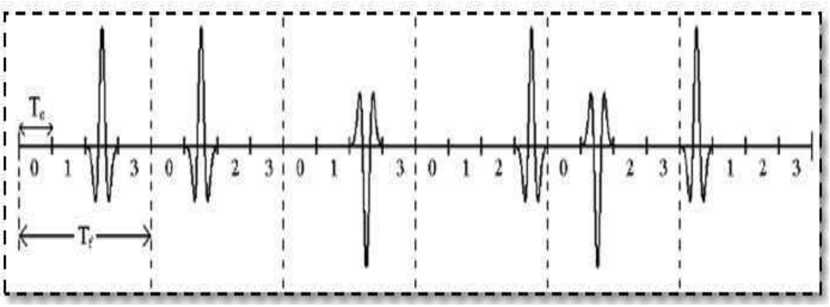


Figure 2.12 – *radio pulses generated by UWB*

  - The UWB signals have a low power spectral density (Figure 2-12) ; since the signal is
  - It provides a broad frequency band and varies between 3.1 GHz and 10.6 GHz [34] : (Figure 2-13) ; spread over a wide bandwidth. This feature gives the UWB systems using a low probability of detection and interception ;
  - The ultra wide band signals interfere with few or no other signals such as narrowband signals, because their power is very low on the small part of the spectrum concerned. So, using this type of signal allows more security. UWB does not suffer from multipath effects, because the direct path arrives well before the cancellation with local roads will occur ;
  - The ultra wideband signals have good penetration capabilities probably due to their large bandwidth. They can pass through surfaces such walls, unlike other technologies. They are used in the case of UWB radar in nondestructive testing of structures (cavities above the vaulted tunnels, detecting mines buried etc.) ;
  - The ultra-wideband signals to allow for high precision in the measurement of distances, because the resolution is inversely proportional to the duration of the pulse.
  - UWB also allows better energy saving compared to other technologies [35] (Figure 2-14) ;

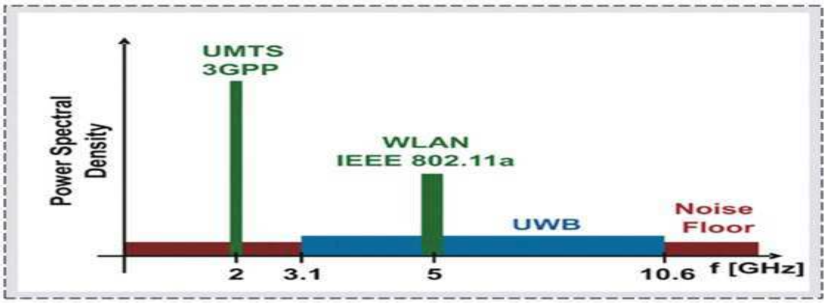


Figure 2.13 – *Positioning of the UWB frequency and the energy spectral density.*

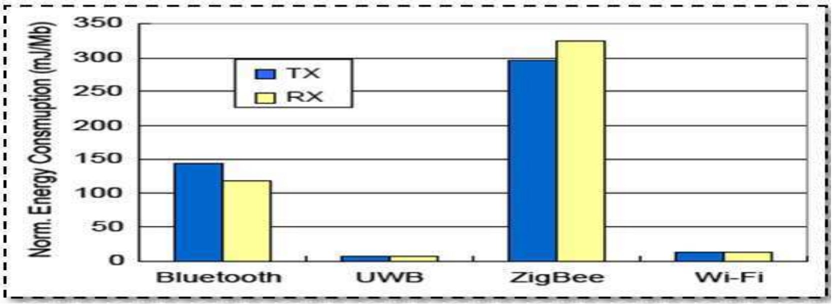


FIGURE 2.14 – *Comparison of Energy Consumption in some Standards*

- ○ Offer better throughput suitable for sending media stream but at a distance(range) very average ;

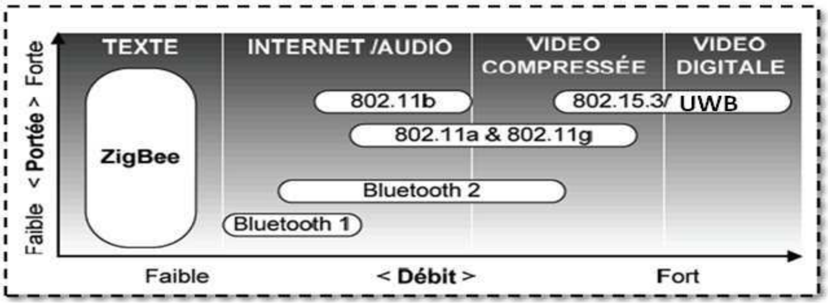


FIGURE 2.15 – *Positioning of UWB to send streaming media*

- ○ Compared to other UWB standards is positioned properly in terms of transmission speed and mobility which can read several more applications to use as a reliable solution.

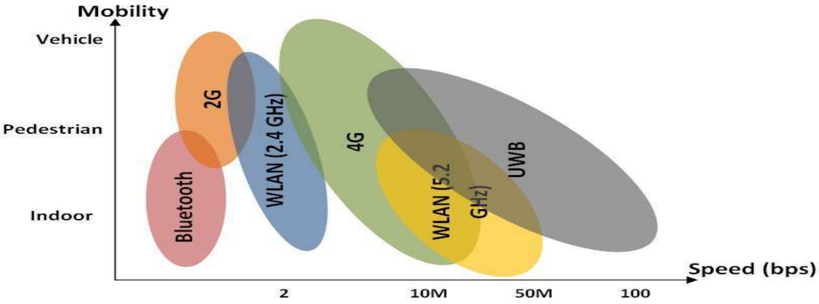


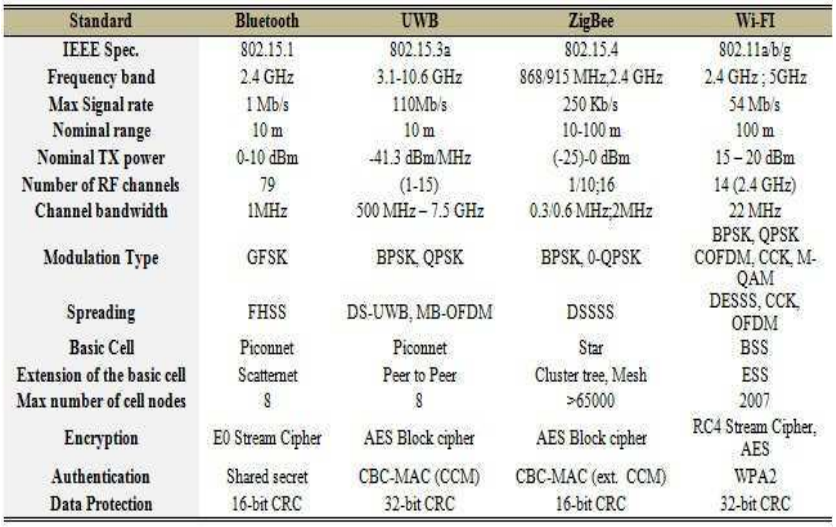
FIGURE 2.16 – *Positioning technologies based on the speed and mobility*

Table → (Figure 2-17), [35], below summarizes the characteristics of wireless technologies, Bluetooth, ZigBee and UWB and presenting a comparison between them as reliable solution :

. UWB Applications

Many applications use UWB technology, and benefit from these important advantages, among these applications are cited :

- ○ Desktops ,laptops, printers, scanners ;
- ○ Mobile and multimedia files, MP3, games, video ;
- ○ Personal Connectivity Camera, DVD player (Figure 2-18)
- ○ Positioning, Geo location, location ;
- ○ Obscure Environment ;
- ○ Short-range communication and high speed ;
- ○ Communication with low interference ;



Standard	Bluetooth	UWB	ZigBee	Wi-FI
IEEE Spec.	802.15.1	802.15.3a	802.15.4	802.11a/b/g
Frequency band	2.4 GHz	3.1-10.6 GHz	868/915 MHz,2.4 GHz	2.4 GHz ; 5GHz
Max Signal rate	1 Mb/s	110Mb/s	250 Kb/s	54 Mb/s
Nominal range	10 m	10 m	10-100 m	100 m
Nominal TX power	0-10 dBm	-41.3 dBm/MHz	(-25)-0 dBm	15 – 20 dBm
Number of RF channels	79	(1-15)	1/10;16	14 (2.4 GHz)
Channel bandwidth	1MHz	500 MHz – 7.5 GHz	0.3/0.6 MHz;2MHz	22 MHz
Modulation Type	GFSK	BPSK, QPSK	BPSK, 0-QPSK	BPSK, QPSK COFDM, CCK, M-QAM
Spreading	FHSS	DS-UWB, MB-OFDM	DSSSS	DESSS, CCK, OFDM
Basic Cell	Piconnet	Piconnet	Star	BSS
Extension of the basic cell	Scatternet	Peer to Peer	Cluster tree, Mesh	ESS
Max number of cell nodes	8	8	>65000	2007
Encryption	E0 Stream Cipher	AES Block cipher	AES Block cipher	RC4 Stream Cipher, AES
Authentication	Shared secret	CBC-MAC (CCM)	CBC-MAC (ext. CCM)	WPA2
Data Protection	16-bit CRC	32-bit CRC	16-bit CRC	32-bit CRC

Figure 2.17 – *Characteristics of wireless technologies, Bluetooth, ZigBee, Wi-fi and UWB*

- ○ Telecommunication and Radar (sensors)
- ○ Medicine ;
- ○ The protection and security systems ;
- ○ Rescue systems to detect people buried (Figure 2-19) ;
- ○ Detection of people hidden behind obstacles ;
- ○ Control over the rail yard in yard ;
- ○ The control of air traffic in the canyons ;
- ○ UWB Radar examining the emotional state of patients by heart rate variability.
- ○ Home Automation (Figure 2-20)
- ○ Radar vehicles (Figure 2-21), etc.

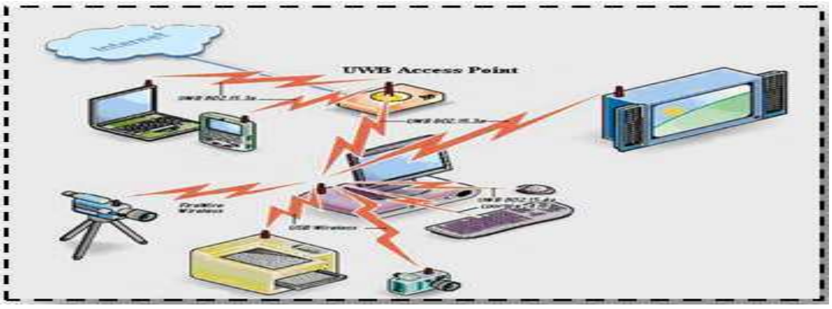


Figure 2.18 – *Connectivity via carrier-based UWB*

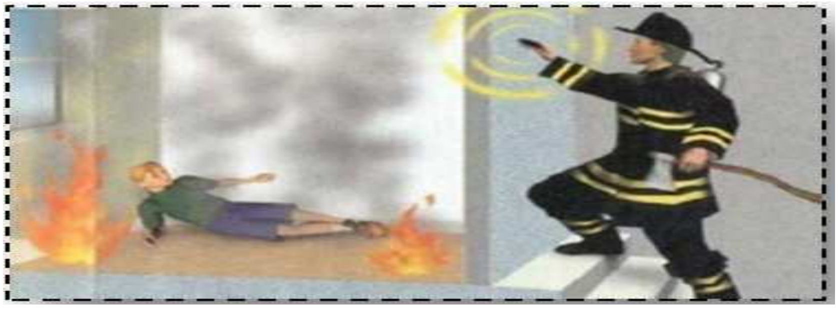


Figure 2.19 – *Using UWB Rescue and Safety*

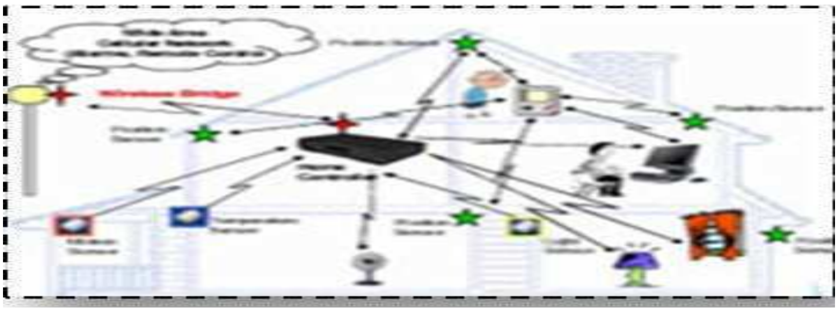


Figure 2.20 – *Use of UWB in the home automation*

Figure 2.21 – *Use of UWB in vehicles*

2.2.5 CONCLUSION

Emerged in these various technologies, WSN have found their flexibility and robustness to capture and transmission, acceptable range though, traditional data namely, temperature, humidity, light, and others. This transmission is based on its physical transmission medium (Physical Layer) protocol stack and operating at the MAC layer, the ZigBee alliance that proved successful in many applications in various fields.

The following section treats and surveys the security challenge in wireless sensor network by listing the several attacks and solutions.

ABSTRACT

"The routing and the QoS are strongly related. In the next we list the pertinent protocols in WSN and give QoS definition and used metrics for the study of the performance of routing protocols in ad hoc and sensor networks."

2.3 QoS and Routing Protocol In WSN

2.3.1 INTRODUCTION

In telecommunication networks, the goal of QoS is to achieve better communication behavior, so that the contents of the latter are correctly routed, and network resources used optimally.

Generally, research on QoS in wireless networks in several key areas ; Models of QoS differentiation at the MAC layer (Medium Access Control), signaling protocols and routing with QoS.

2.3.2 CONCEPT OF QUALITY OF SERVICE

The QoS (Quality of Service), [26], can be defined as the degree of satisfaction of a user of services provided by a communication system. QoS is defined as the ability of a network element (eg router, node or application) to provide a level of security for a data flow.

RFC 2386 QoS features as a whole needs to be provided by the network to transport traffic from one source to a destination. These needs can be translated into a set of attributes pre-specified and measurable in terms of :

- End to End delay,
- Variance of delay (jitter),
- Bandwidth,
- Packet losses.

Depending on the application, the QoS requirements (Figure 2-22) are different. For example, for real-time applications like voice and video (multimedia), the time from start to finish of a package must be limited, otherwise the package is useless. Other wireless applications focus on the life of the network which is a function of the energy consumed and the security of communication which are in high demand sensor networks in particular. [27].

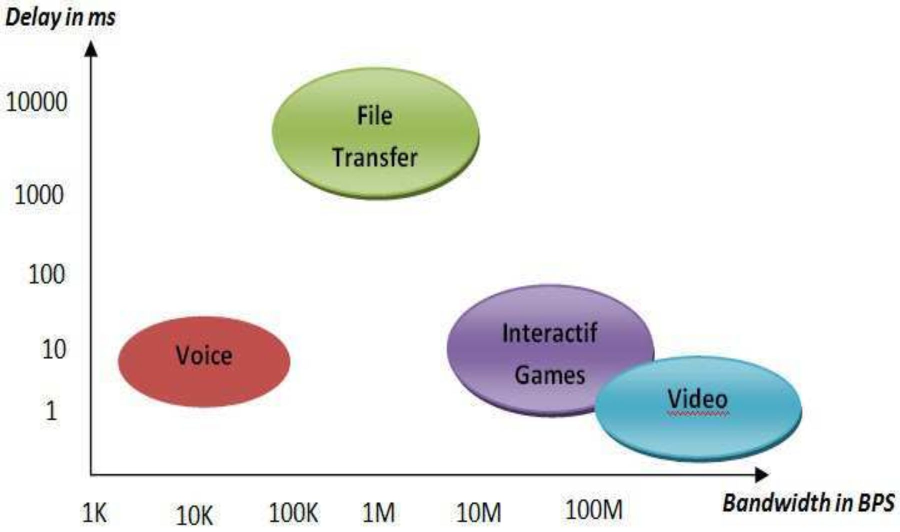


Figure 2.22 – *Sample Quality of Service requirements*

2.3.3 THE METRIC OF QUALITY OF SERVICE

The major known aspects of service quality [28] are : bandwidth, end to end delay, jitter (delay variation) and packet loss (often expressed in terms of error rate).
QoS metrics can be additive, multiplicative or concave ; [27].

- Additive metric Am is defined as where $\sum_{i=0}^{h} Li(m)$ is the value of the metric m on the link Li, $Li \in P$ while h represents the length of the path P.
- Concave metric defines the minimum value on a path P and represented as follows : $min(Li(m))$, $Li(m) \in P$.
- Multiplicative metric is the product of the values of QoS metrics, it is defined as the product of $Li(m)$ with i from 1 to h, $Li(m) \in P$.

The Bandwidth is a concave metric, while the delay and jitter are additive metrics. The availability of a link, based on criteria such as the probability of loss of link on it is a multiplicative metric.

- The usual metrics in QOS :
- ○ The bandwidth
  Bandwidth is occupied by the transmission source or receives a flood. Management of bandwidth is an important element in ensuring the quality of service.
- ○ End to End Delay
  The term "delay" actually includes three different temporal aspects :
  - ∗ The propagation delay determined by the physical distance between the source and the destination.
  - ∗ Waiting time and the packet processing within the queues, determined by the network load, as well as policy information processing in the routers for maximum smoothness of the flow of information.
  - ∗ The transmission delay depending on the size of the waves. This parameter is closely related to network usage and sharing of available bandwidth. Guarantee period, implies the need to implement mechanisms to better manage the flow of information to the destination in minimum time, considering the three types of delays mentioned above.
  - ○ The jitter (delay variation)
    Jitter is the variation in transmission delay between end to end packages of a different flow through a network. Jitter is mainly due to delays in processing variables in the network nodes. This setting automatically at night to quality of service requested.
  - ○ Packet loss
    It occurs when there are errors on data integrity. Packet loss occurs mainly when the traffic intensity on the links output becomes greater than their ability to flow. As can calculate the rate of packets delivered (TPD) as follows :

$$TPD(\%) = 100x\frac{\sum \text{Received Packets}}{\sum \text{Sent Packets}}$$

  - Energy management in WSN :

As described in [27], power management in such networks is crucial because the sensors have severe energy constraints. In fact, the limited energy capacity sensors dictate the mode of communication within the wireless sensor networks. Therefore, the protocols designed for WSN must wisely use the finite energy resources. Design protocols taking into account energy consumption becomes crucial for the establishment of a viable WSN. In this regard, use of effective techniques optimizing energy consumption is essential to achieve significant energy savings in a WSN.

Ideally, a communications protocol for WSN sensors must operate only when needed. Otherwise, all sensors must be in sleep mode. Furthermore, when communication is established, no redundant data should be transferred. In addition, the traffic should be distributed equitably among the sensors to avoid congestion and premature death of the network. So we need to operate only at the right time right sensors to transmit useful data only through the best path.

Unfortunately, such an optimal configuration is not feasible since it requires a preliminary knowledge of the model traffic generation and network topology. Therefore, research is oriented towards the concept of efficiency of energy use (as opposed to the notion of optimality). Efficiency can be defined as maximizing the lifetime of the network as long as possible.

2.3.4 ROUTING PROTOCOL WITH QUALITY OF SERVICE

The principle of routing with quality of service is to seek a path between two nodes satisfying certain constraints. The metrics listed above can be used (delay, bandwidth, or the cost of transmission). Depending on the type of constraints, finding optimal routes may become a problem. Routing with quality of service usually adds to routing protocols usual admission control to select among the available routes those that satisfy the constraints of the flow. The main problem with this type of protocol is the extra cost.

The traditional routing algorithms have been proposed to route data without regard to specific constraints or user requests. Thus, they are unsuitable for applications that require the support of QoS.

The QoS routing is a key element to achieve QoS architecture for sensor networks. The QoS routing protocol may inform a source about the bandwidth and availability (in terms of QoS) of the destination. This knowledge will enable the establishment of connections with quality of service.

The following figures (figure 2-23), [27], illustrate the difference between a standard protocol and a protocol with QoS :

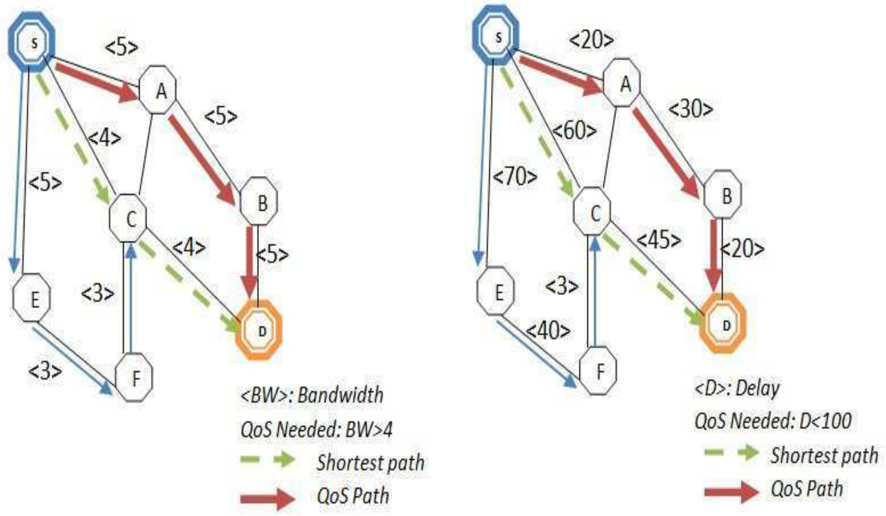


FIGURE 2.23 – *Example of difference in choice of QOS*

Routing protocols in WSN

Propagation and delivery of data in a WSN are the most important feature of the network. It must consider all sensor characteristics and meeting the requirements of the quality of service (QoS) to ensure the best performance of the system life, reliability, response time, etc. Given the specificity of WSN, a large number of research is oriented towards a violation of layering protocol independent, and introduce the concept of cross layer optimization. For example, using aggregation mechanisms, intermediate routers need to access the data to prepare summaries of readings in the region.

- Classification of routing protocols

Recently, routing protocols for WSN have been widely studied, and various studies have been published. The methods can be classified according to several criteria as shown in the figure 2-24 [17] :

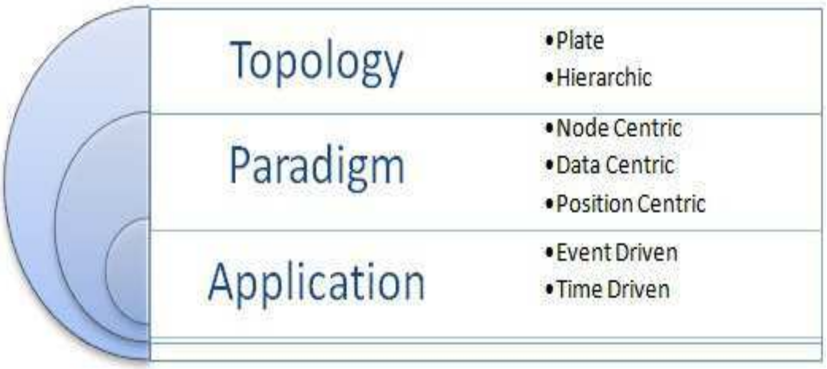


FIGURE 2.24 – *Classification of Routing Protocols*

○ Network topology :

- The topology determines the organization of sensors in the network. There are two main topologies in routing protocols for WSN. Topology plate : a flat topology, all nodes have the same role. Nodes are similar in terms of resources.

  - The hierarchical topology : to increase the scalability of the system, hierarchical topologies have been introduced by dividing the nodes into several levels of responsibility. One of the most common methods is clustering, where the network is partitioned into groups called "clusters". A cluster consists of a leader (cluster-head) and its members.

○ Communication Paradigm :
In WSN, there are three communication paradigms :

  - Node centric : this paradigm is that used in conventional networks, where communications are based on the identification of participating nodes, which is done using IP addresses.
  - Data centric : in a WSN, the data is more important than the node itself, making its identification unnecessary. In the data centric paradigm, the communicators are identified by their data, and therefore the entire system (routing, query, etc.) Must be governed by this property. Thus, the system can be viewed as a distributed database, where the nodes form virtual tables, supplied by the data collected.
  - Position centric : in this approach, the positions of the nodes represent the primary means of addressing and routing. In some applications it is more interesting to query the system using the positions of nodes, their IP addresses. In this case, routing is done using geometric techniques to route information from one geographic area to another.

○ Type of Application :
The method of capture of data in a WSN depends on the application and the importance of the data. Therefore, the WSN can be categorized as time-driven or event-driven.

  - Application time-driven : a time-driven network is suitable for applications that require periodic data collection. For example, it is useful in monitoring applications (fire weather) to prepare periodic reports.
  - Application event-driven : in real-time applications, the sensors must react immediately to sudden changes of sensed values. A periodic collection of data is inadequate for such scenarios. For this, the protocol must be reactive and must give quick responses to the occurrence of certain events.

○ Examples of routing protocols in WSN :
Several constraints must be taken into account in the design of WSN[29] and [17] :

- Constraints energy : all layers must consider the limitation of energy to maximize the lifetime of the network.
  [•] Bandwidth.
  [•]Lack of global addressing
  [•]Redundant Data
  [•]Network multiple source / single destination
  [•]Resource Management
  [•]Capacity Calculation
  [•]Storage

▷ The SPIN Protocol

Heinzelman et al. have proposed a family of protocols called SPIN (Sensor Protocols for Information via Negotiation) [30], based on a negotiation model to propagate information in a sensor network. The purpose of SPIN is to overcome the problems of flooding, which are :

→ The implosion due to duplication of receptions of the same message.

→ The overlap of deploying dense sensor. Using the flood zone sensors will issue all the same data (or almost).

→ Lack of awareness of resources, because the flooding does not take into account the resources of nodes. These three problems greatly affect the life and network performance. To solve them, SPIN adopts two principles :

→ Negotiation : to avoid the problem of implosion, SPIN precedes the emission of a given by its description using the concept of metadata. The receiver will have the option later to accept the data or not. This mechanism can also solve the problem of overlap.

→ Adaptation resources : a continuous manner, nodes monitor their energy level. The SPIN protocol adapts its execution after the remaining energy of the sensor, and amends the node's behavior.

▷ The SPIN Operations

Communications in SPIN follow three steps (Figure 2-25) :

→ When a node wants to transmit a given, it will first ADV message containing a description of the data in question.

→ A node receiving ADV message, checks its basic interest. If interested in this information, it sends a message REQ to its neighbor.

→ Receiving a message REQ, the transmitter transmits to the person given as a DATA message.

The following figure illustrates these three steps [30] :

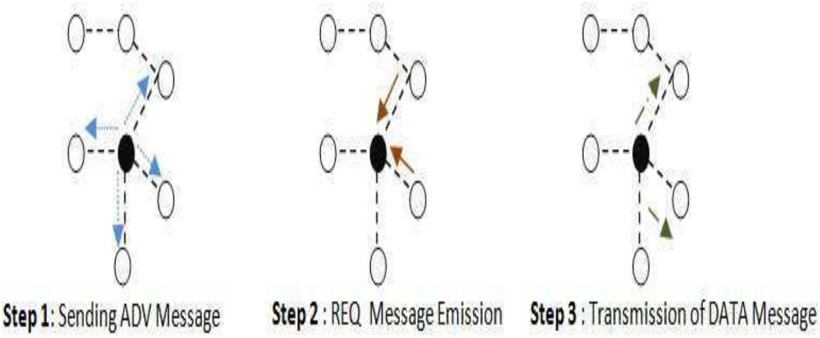

Step 1: Sending ADV Message
Step 2 : REQ Message Emission
Step 3 : Transmission of DATA Message

Figure 2.25 – *Spin Operations and steps*

▷ Directed Diffusion Protocol

Directed Diffusion is a protocol for data propagation, allowing multiple paths for routing information. The sinks diffuse interest (figue 2-26) as a query to look for a particular data in the network.

It is based on the model publish / subscribe DD based on four elements [17] :
→ Data nomination,
→ Interest propagation and establishment of gradients ;
→ Data propagation ;
→ Building routes

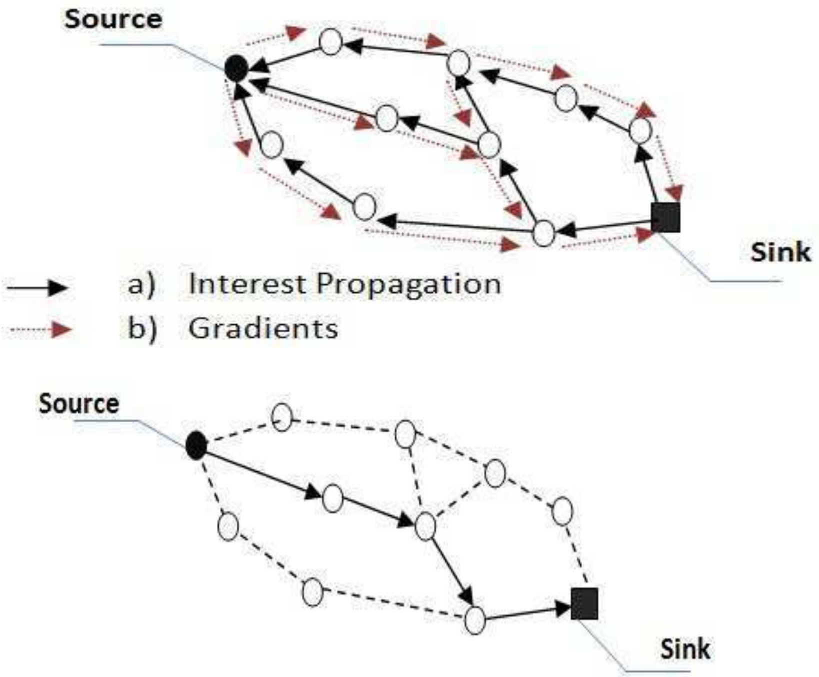


FIGURE 2.26 – *Interest spread and establishment of gradients and Builing roads*

▷ The MCFA Protocol : Minimum Cost Forwarding Algorithm
Ye et al. proposed algorithm MCFA (Minimum Cost Forwarding Algorithm), searching a minimal path between source and sink, while considering the limitations of sensor networks. The protocol aims to achieve three main goals :
→ Optimality : by routing data paths at minimum cost.
→ Simplicity : resulting in low memory consumption, and non need for identifying nodes.
→ Scalability : given the low memory consumption and the absence of node identifier.
The protocol can be used for a large number of nodes. In addition, the phase of road construction consumes one message per sensor. Each node maintains a variable cost, which determines the minimum cost to the wells on the optimal path. Several measures can be used, depending on the desired application : hop count, energy consumption, etc.
The algorithm proceeds in two phases costing relay packets.
▷ Rumour Routing Protocol
Previous protocols use some form of flooding to the spread of interest or data. Rumour routing protocol tries to find a compromise between the interests of flooding and the spread of data.
→ Principle :

The authors used a probabilistic method, based on the following fact : Simulations based on the Monte Carlo showed that the probability that two lines cross within a rectangular region is 0.69. In addition, when using 5 lines through a point, the probability that another line intersects one of the five lines is 0997 ! Therefore, if one considers the source as well and the two points, and establishing a limited number of half-way from the source and sink, we will have a strong chance that two half-paths join, creating a complete path between the source and destination, while avoiding the flood. The creation of these mid paths is based on the notion of agent. An agent is a package with a wide range (TTL) which traverses the network from node to node to establish tables over. There are two types of agents :

- ▷ Event Agent (EA) ; Each node maintains a table of local relay, which contains, for every interest, the next hop to the sink and to the source, and a metric that represents the number of hops to each end. When a node observes a new event, it creates a new agent after a certain probability. The agent contains the table of events in the path traveled and the number of hops to the source of each event (Figure 2-27). In addition, the officer must carry with him the list of nodes examined and their immediate neighbors. The source chooses a random neighbor and sends him the agent.

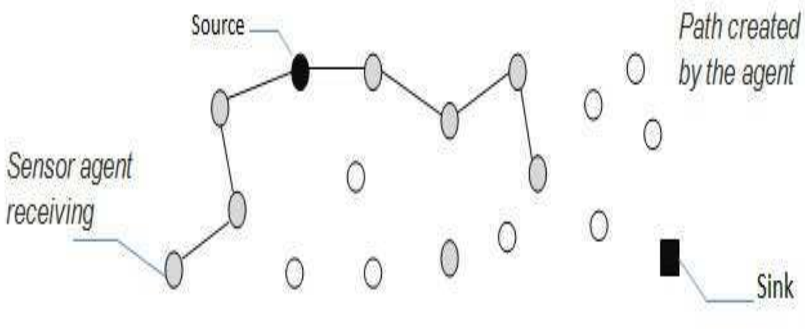


Figure 2.27 – *Agents envents*

- ▷ Query Agent (QA). When the well wishes to take a given network, it checks its local table for a fresh way. If no entry is found, it initiates a request agent. The agent contains only the list of nodes visited. When a node receives a request agent, it checks the existence of a path in its local table. If this is not the case, it chooses a random neighbor and sends the agent, while adding its identifier in the list carried by the agent.

▷ Protocol CPEQ

In addition to all the mechanisms of fault tolerance that implement PEQ, variant CPEQ (Cluster-based PEQ) adds a module clustering to provide better routing management. Indeed, the nodes with more residual energy are selected as aggregator nodes (also called cluster head or hub).

An aggregator node sets its cluster, and nodes belonging to the latter send their data to the aggregator who performs any processing on the raw data and then routes them to the collector. Each network node can become aggregator for a certain period of time depending on its battery level. The main purpose of CPEQ is distributed in uniform energy dissipation among nodes, and to reduce latency and data traffic in the network : (Figure 2-28)

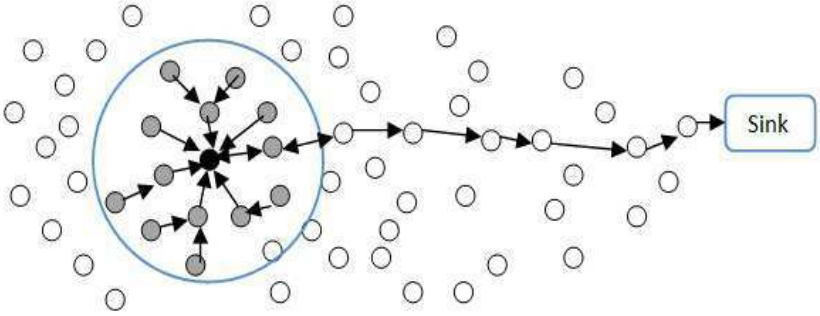


Figure 2.28 – *Data Transmission to the collector*

▷ LEACH : Low-Energy Adaptive Clustring Hierarchy
LEACH [20] (Low-Energy Adaptive Clustering Hierarchy) is a hierarchical routing protocol, employing a method of clustering which divides the network into two levels : the cluster-heads and member nodes. The protocol proceeds in rounds. Each round consists of two phases : construction and communication.

▷ Construction Phase : The purpose of this phase is the construction of clusters in choosing leaders and establishing policy media access within each group. This phase begins with the local decision making to become cluster-head. Each node chooses a random number n, if this number is less than a value T (n), the node becomes cluster-head.

▷ Communication Phase : Using the TDMA schedule, members transmit their data captured during their own slots. This allows them to turn their communication interface outside their reserved slots in order to save energy. This information is then aggregated to be forwarded to the collector (sink).

▷ TEEN : (Threshold sensitive Energy Efficient sensor Network protocol)

Using TDMA, the LEACH protocol is designed for time-driven applications. In this application, the data is propagated in a periodic fashion. However, this kind of protocol is not suitable for event-driven applications, where a reactive behavior is necessary for proper system operation. [31] TEEN (Threshold sensitive Energy Efficient sensor Network protocol) was developed to model LEACH to meet the requirements of event-driven applications. The majority of TEEN behavior is similar to LEACH protocol. However, some differences exist. Elected leaders do not transmit a TDMA schedule, but emit a message containing the following information :

Attributes : represent the assigned task to the sensor.
Hard threshold (HT) : determines the critical value after which the members should send their data reports.
Soft threshold (ST) : specifies the minimum change forcing the node to send a new report.

So when a node realizes that the value captured HT exceeded, it must issue a report to the head. Retransmits it to a new report that if the value changes dramatically, ie : the difference exceeds ST. This mechanism allows implementing a reactive behavior, while limiting the number of messages used.

▷ SAR (Sequential Assignment Routing)

SAR is multi-paths that strive to achieve energy efficiency and fault tolerance. SAR trees creates taking into account the QoS metric, the energy source on each path and the priority level of each packet. Using these trees, multiple routes to the sink sensors are formed. One or more routes can then be borrowed.

▷ SPEED

The protocol requires that each node maintains information about its neighbors. It proceeds by geographic routing nodes to select next hops to reach the final destination Sink. In addition, SPEED ensures packet delivery rate constant, denoted SetSpeed. This ensures delivery times from start to finish acceptable. These periods may be estimated by dividing the distance between the source nodes by the sink speed SetSpeed.

2.3.5 CONCLUSION

Propagation and routing data in a WSN is seeking a better quality management of its service metrics to ensure the best system performance. Why routing in WSN is a complex problem. Thus, the design of a routing protocol is based on factors that must be met to achieve effective communication. The satisfaction of these factors can be measured by parameters to test the performance of the routing protocol after its completion.

Several routing protocols have been proposed for WSN due to their advantages. Although routing techniques appear promising, they remain a subject to overcome a significant challenge to know that security communication. Thus, the next chapter will be devoted to the issue of trade security in WSN as well as solutions that bring about the various threats and risks.

The next section if focused on the politics of security in WSN. It gives an overview on the security mechanism adopted for assuring the communication between sensors.

ABSTRACT

"The security issue is a ubiquitous problem in wireless communication. WSN have a vast part of this problem due to his vulnerability to several attacks. The following section approaches the reader to the existing attacks and solutions in this field."

2.4 Security In WSN : A Survey

2.4.1 INTRODUCTION

Communication between sensor nodes is the subject of ongoing research to improve its performance. But beyond this issue, other issues begin to appear as a guarantee of safety communication. Indeed, the network is dedicated to monitoring properties for intrusion detection or risk areas where information is transmitted downstream used for making important decisions. A research team has recently shown that some medical equipment (defibrillators in this case) do not contain any security mechanism and can be easily abused. An attacker can disrupt, or simply stop the defibrillator to a victim, thus endangering human life.

This chapter discusses the security issues in WSN that differ from other networks in that they offer greater restrictions in terms of energy, processing capabilities and communication. We will begin to investigate the threats against the WSN. Subsequently, we will study the basic services of the safety procedures to avoid these threats and describe the various mechanisms to provide these services.

2.4.2 SECURITY TRADE IN WSN

The properties of sensor networks are double-edged. While they allow ease of production and deployment, but make the overall system of communication rather "fragile" to a number of failures [17].

To ensure broad deployment of this technology, it is necessary to address these safety issues at different levels of WSN architecture.

SECURITY PROBLEMS :

The main security issues in WSN emerge from the properties that make them efficient and attractive, which are :

- **Limitation of resources :** energy is perhaps the greatest constraint to the capacity of a sensor node. The stored energy of each node must be kept to prolong its life and as well as that of the entire network. In most cases, the information transmitted is seen as redundant sensors are usually geographically co-located. Most of this energy can be saved through data aggregation. This requires special attention to detect the injection of false data or modifying defective data during aggregation operations at intermediate nodes.
- **The wireless multi-hop :** in addition to providing a simple deployment, wireless communication has the advantage of providing access to hard to reach areas such as land and disastrous hostile. Unfortunately, the scope of the radio communication of "motes" is limited due to energy considerations. Multi-hop com-

munication is essential for the dissemination of data in a WSN. This introduces many security holes at two different levels : attack of the construction and maintenance of roads, and attack payload injection, modification or removal of packages. In addition, wireless communication introduces additional vulnerabilities to the link layer, opening the door to attacks and jamming style denial of service by depletion of batteries.

- **Close coupling with the environment :** most of WSN applications require a tight deployment of nodes within or near the phenomena to be monitored. This physical proximity with the environment leads to frequent intentional or accidental compromise of nodes. As the success of WSN applications also depends on their low cost, nodes cannot afford physical protection inviolable. Therefore, an adversary "well equipped" can extract cryptographic information of sensor nodes. As the mission of a WSN is usually unattended, the potential of attacking nodes and retrieve their content is important. Thus, cryptographic keys and sensitive information should be managed in a way that increases resistance to capture nodes.
  The figure 2-29, [17], summarizes the security issues emerging from the characteristics of a WSN and solutions to be undertaken :

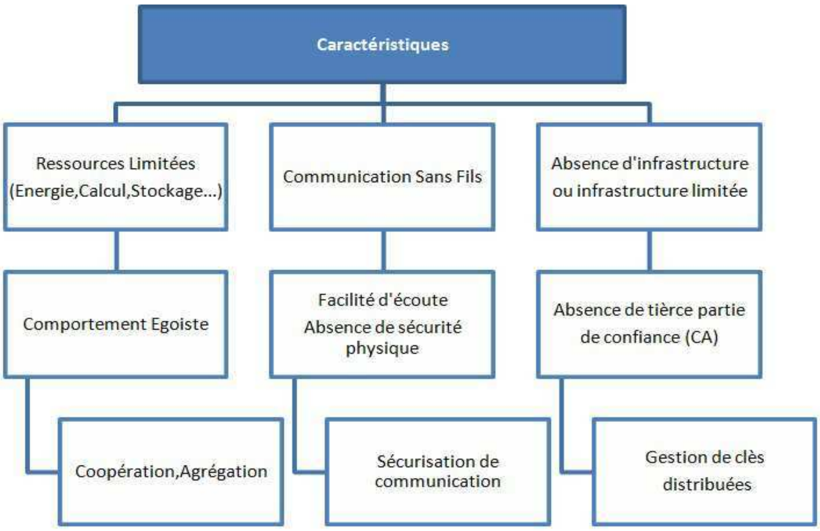

Caractéristiques
Ressources Limitées (Energie,Calcul,Stockage...)
Communication Sans Fils
Absence d'infrastructure ou infrastructure limitée
Comportement Egoiste
Facilité d'écoute Absence de sécurité physique
Absence de tièrce partie de confiance (CA)
Coopération,Agrégation
Sécurisation de communication
Gestion de clès distribuées

FIGURE 2.29 – *Problems and security solutions in WSN*

LOCKED FUNCTIONAL SECURITY IN WSN

As shown in the figure 2-30 below, there are four functional blocks of security solutions in WSN [17] :

- Key management, (Figure 2-32)
- The security of routing,
- Security of data aggregation,
- The safety of access to the channel.

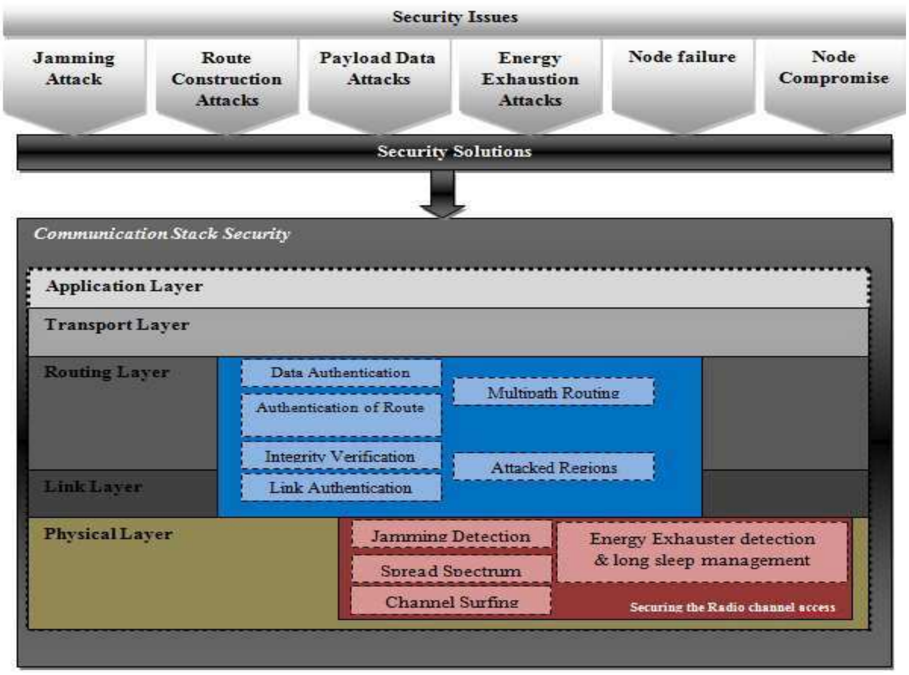


Figure 2.30 – *Functional blocks in security solutions in WSN*

KEY MANAGEMENT

Key management, [17], is one of the most difficult aspects of configuring a cryptographic system security. For such a system works is to be secured, each user must have a set of secret keys (in a secret-key) or key pair public / private (in a public key system) (Figure 2-31).

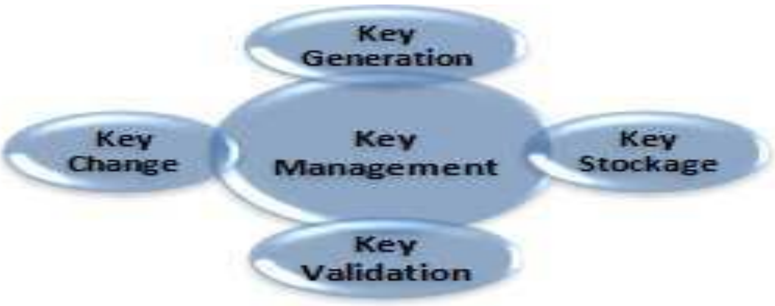


Figure 2.31 – *Key management in WSN security*

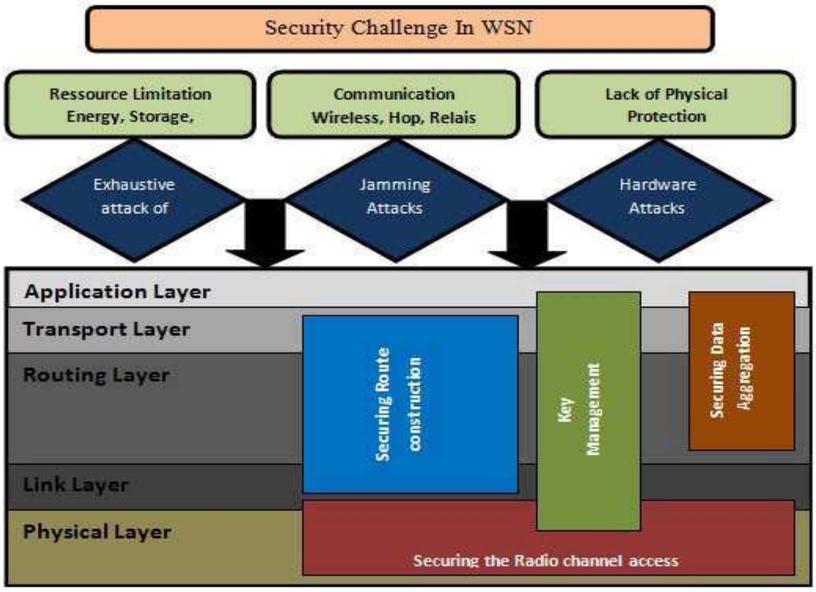

Security Challenge In WSN
Ressource Limitation Energy, Storage,
Communication Wireless, Hop, Relais
Lack of Physical Protection
Exhaustive attack of
Jamming Attacks
Hardware Attacks
Application Layer
Transport Layer
Routing Layer
Link Layer
Physical Layer
Securing Route construction
Key Management
Securing Data Aggregation
Securing the Radio channel access

FIGURE 2.32 – *Deployment and key management for sensor*

KEY MANAGEMENT PROTOCOLS

The protocols are classified according to the way in which neighboring nodes share common keys (probabilistic or deterministic) (Figure 2-33), and according to the network topology (hierarchical or flat) [17] :

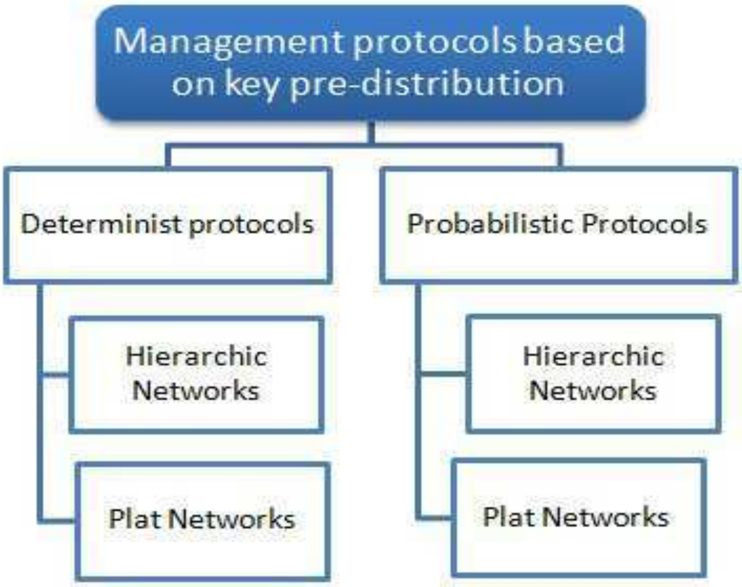


FIGURE 2.33 – *Key management protocols in WSN*

∗ Protocol pre-key distribution and L.ESCHENAUER D.GLIGOR Eschenauer and Gligor proposed a key management scheme based on the probability of sharing a key between the nodes of a random graph. It provides techniques for pre-key distribution, the discovery of the shared key, the establishment of key path, and key revocation. The thrust of this scheme is to randomly distribute a number of keys, from a finite set at each network node before deployment. Any two nodes will be able to exchange secure messages if they have a common key.

* The LEAP Protocol
  LEAP is a deterministic protocol for key management for sensor networks Wireless. The key management mechanism provided by LEAP Support internal processing "in-network processing" while limiting the impact of security by a compromised node on its neighborhood in the network. LEAP Support the establishment of four types of keys for each node (individual key, pair key, group key or global key).

2.4.3 ROUTING AND SAFETY IN WSN : THREATS AND SOLUTIONS

Seen the constraints of WSN, most routing protocols are quite simple, and therefore quite vulnerable to attack. A malicious node can operate on two levels :
* The data exchanged between the nodes ;
* The network topology created by the protocol.

These attacks can be classified into two categories : active and passive.

ACTIVE ATTACKS

* **Attack "jamming"**
  Given the sensitivity of wireless media noise, a node can cause a denial of service by issuing signals at a certain frequency. This attack (Figure 2-34)can be very dangerous because it may be conducted by a non-authenticated and foreign network. [17] :

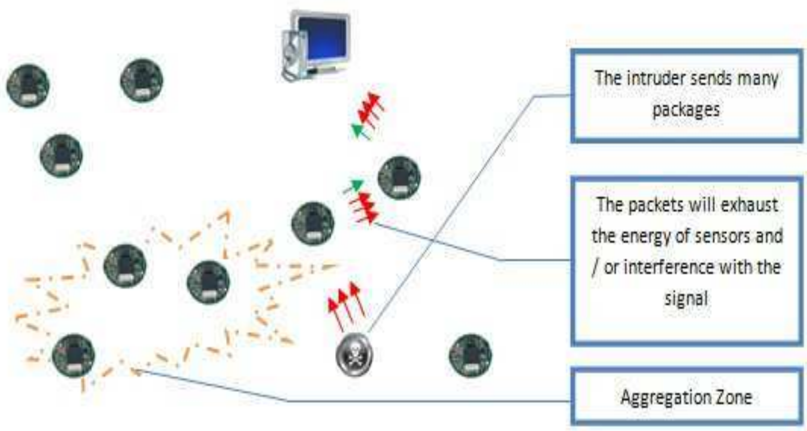

The intruder sends many packages
The packets will exhaust the energy of sensors and / or interference with the signal
Aggregation Zone

FIGURE 2.34 – *Jamming Attack*

* **Attack Sink hole** In a sink hole attack, the node tries to attract him to the most possible ways to control over most of the data flowing through the network. To do this, the attacker must appear to others as very attractive, presenting optimal routes (Figure 2-35). [17]

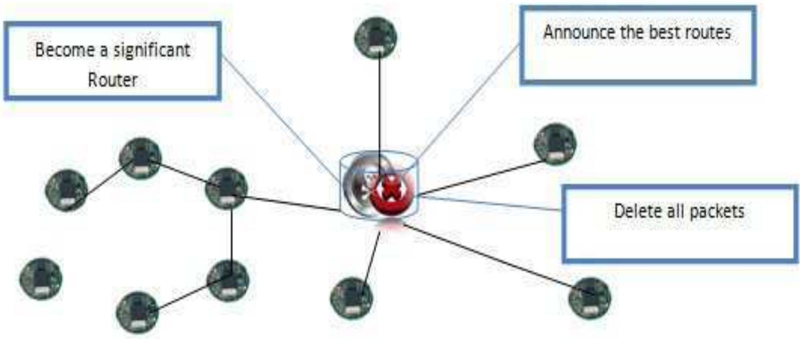


FIGURE 2.35 – *Sink Hole Attack*

- **Hello Flooding Attack** This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbour. As a consequence, while sending the information to the sink, the victim nodes try to go through the attacker as they know that it is their neighbour and are ultimately spoofed by the attacker (Figure 2-36).

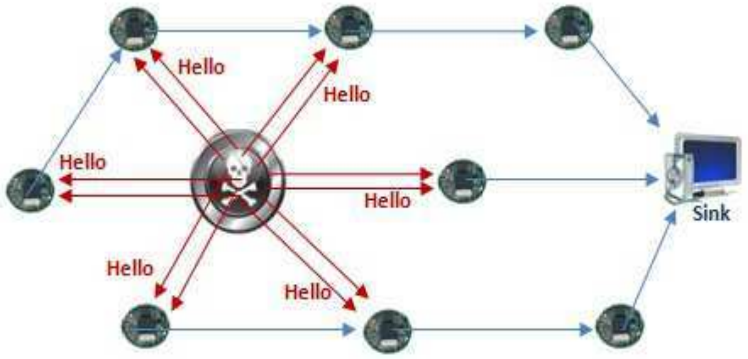


FIGURE 2.36 – *Hello Flooding Attack*

PASSIVES ATTACKS

- **Lack of cooperation or Selective Forwarding** All routing protocols assume that nodes are "honest" and will normally pass on the packets passing through them. However, an attacker can violate this rule by removing all or part of these packages. Moreover, if the attacker has previously used a sinkhole attack, it becomes a large router in the network. So, abandoning its role as a router, the performance of the systems will be severely degraded.
- **Eavesdropping (Listen For)** As the wireless medium is an open medium, a node can hear all communications from its neighbors. This can disclose important information, such as the lo-

cation of an important node. The combination with a sinkhole attack worsens advantage of the impact of this attack.

TYPES OF SOLUTIONS

We distinguish three levels of solutions to the attacks on routing data in WSN :

∗ **Prevention against active attacks :**
In this category are generally used cryptographic mechanisms to protect the signaling used to build roads. It is generally mechanisms for authentication and integrity check that is used to prevent a malicious node to inject, modify and/ or delete information that will be used for the discovery, construction or maintenance of a road.

∗ **Detection of suspicious behavior :**
This category seeks to identify behaviors that reflect a passive attack (lack of cooperation, refusal to relay packets, etc.).

∗ **Tolerance :**
In this category, we introduce mechanisms for fault tolerance of nodes due to attacks or failures. The multipath routing is a typical example.

∗ **Security Protocols :**

▷ **SecRoute :**
SecRoute protocol is a protocol for secure hierarchical routing. The network is organized into clusters, each with a leader. The collector node is supposed to know this organization's network, and must maintain a local table with a secret key of each sensor. This key is supposed to pre-loaded into each node. In addition, each cluster must have a key to secure intra-cluster. This key must be known by the cluster-head and all nodes in the group. SecRoute protocol does not specify the algorithm to build clusters, and assumes that the clusters and their keys are established by another protocol such as LEAP.

▷ **SecRoute protocol has the following properties :**

- The routing packets are not large because they contain only-partial information about the progress.
- The protocol uses a two-tier architecture, in which heads aggregate the member data and transmit them to the collector node.
- The protocol uses only symmetric encryption methods.
- For security reasons, the protocol replaces unicasts by targeted broadcasts. Indeed, avoiding unicasts a message sent is received by all neighbors. So it allows to verify, when the relay, the integrity of the message sent by the next hop.

▷ **SAWN (Secure Aggregation for Wireless Networks)**
SAWN assumes that two consecutive nodes cannot be compromised simultaneously. It is based on the audit for two jumps : a node checks whether the aggregation of his small son, realized through his son, is correct. Verification of the aggregation is done in a manner differed in time using the

protocol μTESLA to authenticate keys used in authentication of data and their aggregations.

2.4.4 CONCLUSION

Most important issues of security in WSN are listed in this section, attacks that are increasing, basic services, and prevention mechanisms that encourage the most commonly used to develop a large number of works research.

Several observations are worth noting as the impact of the binding characteristics of WSN on security techniques. Indeed, the WSN take into account the limitation of resources as a first design goal established putting away more advanced mechanisms. In addition, numerous problems remain difficult as the complexity of encryption algorithms, the defense against threats that exploit vulnerabilities in the network, etc.

This problem becomes increasingly attractive in wireless communications where the radio waves that transmit information, based on various technologies, are exposed to these various threats.

The Next Chapter will be focused on the realized works and contributions which explain and summarizes the results found on different axes. This Chapter is divided on five sections giving solid solutions. It describes the functionalities of technologies emerged in WSN communications, security, routing and localization in WSN, and proposing architectures to solve and improve energy consumption in several applications.

3 CONTRIBUTIONS & PRODUCTIONS

ABSTRACT

"This chapter describes a technology function of the sensor network. It gives a performance comparison of two technologies (ZigBee and UWB) with an application in WMSN"

3.1 The UWB Solution for Multimedia Traffic In Wireless Sensor Networks

3.1.1 Introduction

The establishments of wireless networks in various domains know an amazing success. In front of this progress several researches are followed to enlarge the range of its use. Networks of wireless sensors are a particular Ad hoc network, integrated with an active applications allowing control, surveillance and help to decision.

The introduction of wireless communication is dramatically changing our lives. The ability to communicate anytime anywhere increases our quality of lives and improves our business productivity. The recent technological developments that allow us to execute bandwidth-hungry multimedia applications over the wireless media add new dimensions to our ability to Communicate. Various technologies appeared in sensors networks and assure the communication differently, this difference comes especially in the given quality of service and solutions given to constraints.

In this section, we study this functionality in term of the quality of service of technologies ZigBee and UWB (Ultra Wide Band) as well as the consumption of energy for a multimedia flux using the simulator NS2.This to solicit the adapted technology to the transmission of Multimedia flux in WMSN(Wireless Multimedia Sensor Network).

3.1.2 RELATED WORKS

Several papers focused their works on WMSNs treating an enormous topics related to energy efficiency, QoS, routing protocols on MAC and physical layers. Karapistoli et al [36] identify the cross-layer dependencies between the specified physical layer and the higher layers of the communication. In [37] authors raise a ranging method of localization technique in WSN based on ultra-wideband (UWB) communication technology. Melodia et al [38], present a cross-layer communication architecture based on the time-hopping impulse radio ultra wide band technology to deliver QoS to heterogeneous applications in WMSNs, by leveraging and controlling interactions among different layers of the protocol stack according to applications requirements. Berthe et al [39], propose a WSN simulation architecture based on the IR-UWB technique. At the PHY layer, they take into account the pulse collision by dealing with the pulse propagation delay. They also modelled MAC protocols specific to IRUWB,for WSN applications and propose a generic and reusable sensor and sensing channel model. Most of the WSN application performances can be evaluated thanks to this simulation architecture.

3.1.3 WIRELESS SENSOR NETWORKS

Wireless sensor networks (WSNs) contain hundreds or thousands of sensor nodes equipped with sensing, computing and communication abilities. Each node has the ability to sense elements of its environment, perform simple computations, and communicate among its peers or directly to an external base station or sink (Figure 3-1). The node or mote that needs to operate for a long time on a tiny battery is composed of a processor, a memory, a transmitter/ receiver radio, an embedded system composed of a unit of sensing and a battery (Figure 3-2). This component can be in sleep mode or listen only to the traffic. The unit of transmission is the unit which uses most energy compared to others units constituting a sensor [17].

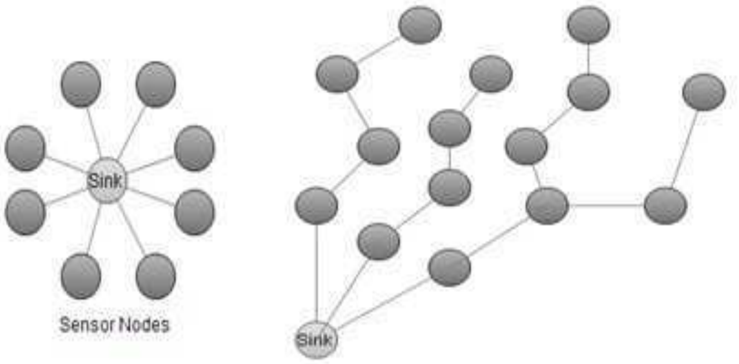


Figure 3.1 – *Architecure of Wireless Sensor Network*

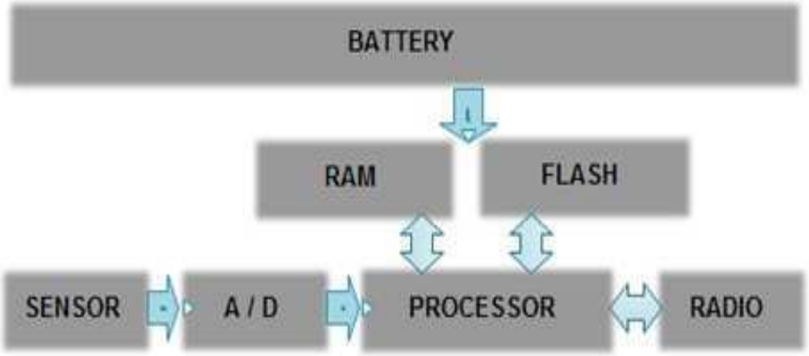


Figure 3.2 – *Node Architecture*

3.1.4 multimedia WIRELESS SENSOR NETWORKS

The technology development in electronics contributed to the availability of miniaturized materials with low cost such as CMOS cameras and microphones which helped more the development of wireless multimedia sensor networks (WMSN), devices that are able to retrieve multimedia content such as the ubiquitous audio and video, still images, and data from environmental sensors. Wireless multimedia sensor networks will not only reinforce the networks of sensors such as monitoring, home automation and environmental monitoring, but will also enable several new applications like monitoring networks multimedia, storage of potentially activities, control systems traffic, medical surveillance environmental monitoring, location services, industrial process control, etc.

3.1.5 THE QUALITY OF SERVICE

In telecommunication networks, the goal of QoS is to reach a better behavior of communication for the content which must be properly routed, and network resources are used optimally [20].

Generally, researches on QoS in wireless networks in several key areas ; models of QoS differentiation at the MAC layer (Medium Access Control) protocols for signaling and routing with QoS. The need of QoS can be specified into measurable parameters mentioned in (3), (4) and (5) :

↪ End to End Delay :

$$EED = \frac{\text{Time spent to deliver packets}}{\Sigma(\text{received packets})}(3)$$

↪ Bandwidth :

$$BW = (\text{packets size})x\frac{\Sigma(\text{received packets})}{\text{End time simulation}}(4)$$

↪ Packet delivery ratio :

$$PDR(\%) = 100x\frac{\Sigma(\text{Received packets})}{\Sigma(\text{Sent Packets})}(5)$$

3.1.6 TECHNOLOGIES EMERGED IN WIRELESS SENSOR COMMUNICATION

Many technologies are allowed to wireless transmission of information. Each represents a different use, according to its characteristics (transmission speed, maximum flow, Cost of infrastructure cost of equipment connected Security, Flexibility of installation and use, power consumption and autonomy, etc.).

ZigBee Technology

ZigBee is a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs), such as wireless headphones connecting with cell phones via short-range radio. The technology defined by the ZigBee specification is intended to be simpler and less expensive than other WPANs, such as Bluetooth. ZigBee is targeted at radio-frequency (RF) applications such as industrial control and monitoring, wireless sensor networks, asset and inventory tracking, intelligent agriculture, and security would benefit from such a network topology that require a low data rate, long battery life, and secure networking.

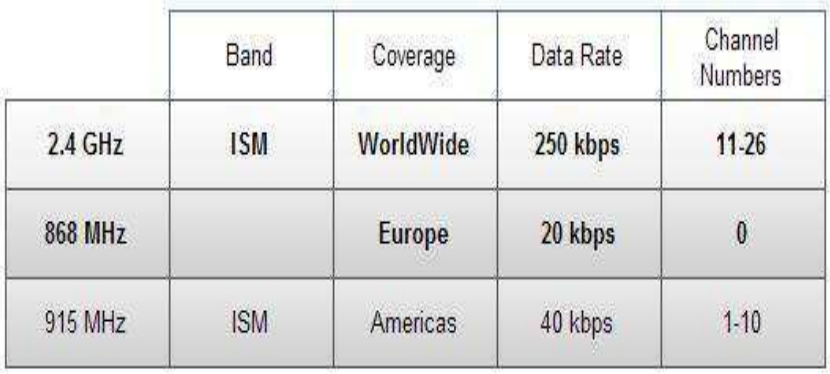
ZigBee builds upon the physical layer and medium access control defined in IEEE standard 802.15.4 for low-rate WPAN's. The specification goes on to complete the standard by adding four main components : network layer, application layer, ZigBee device objects (ZDO's) and manufacturer-defined application objects which allow for customization and favor total integration.

ZigBee operates in the industrial, scientific and medical (ISM) radio bands ; 868MHz in Europe, 915MHz in the USA and Australia, and 2.4GHz in most jurisdictions worldwide. (Figure 3-3)[33].

UWB Technology

Ultra Wide Band (UWB) technology based on sending pulses of energy low power over a wide frequency band is able to communicate wirelessly as an indoor short-range high-speed communication. One of the most exciting characteristics of UWB is that its bandwidth is over 110 Mbps (up to 480 Mbps) which can satisfy most of the multimedia applications, especially in wireless sensor networks, such as audio and video delivery in home networking and it can also act as a wireless cable replacement of high speed serial bus such as USB 2.0 and IEEE 1394. UWB works via chip-based radios that modulate signals across the entire available ultra wideband spectrum, which in the US is from 3.1 to 10.6 GHz (Figure 3-4) [35]. In [40] several standards are mentioned giving the differences among four technologies. Each one is based on an IEEE standard.

Obviously, UWB and Wi-Fi provide a higher data rate, while Bluetooth and ZigBee give a lower one. In general, the Bluetooth, UWB, and ZigBee are intended for WPAN communication (about 10m), while Wi-Fi is oriented to WLAN (about 100m). However, ZigBee can also reach 100m in some applications.



	Band	Coverage	Data Rate	Channel Numbers
2.4 GHz	ISM	WorldWide	250 kbps	11-26
868 MHz		Europe	20 kbps	0
915 MHz	ISM	Americas	40 kbps	1-10

Figure 3.3 – *The three frequencies band for IEEE 802.15.4 standard.*

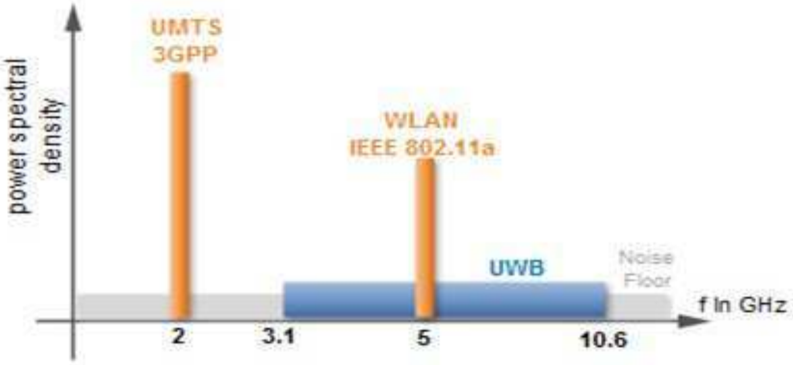


FIGURE 3.4 – *Frequency Spectrum in UWB technology*

3.1.7 SIMULATION AND RESULTS

Environment Of Simulation

The simulation tool used is the NS2 simulator dedicated to wireless networks and considered a crucial asset search.

The version of ns2-allinone-2.29 [10]used, incorporate into the architecture of the MAC layer (mac.cc / mac.h) and physical (phy.cc / phy.h) modules and standard IEEE.802.15.4 supporting radio pulses compliant to IEEE 802.15.3 UWB which adds to its MAC layer modules DCC-MAC layer (mac-ifcontrol*. (cc, h)) and physical layer (interference-phy*. (cc, h)) by implementing the NOAH protocol that allows direct communications (unlike AODV, DSR, etc.) between wireless nodes, or between base stations and mobile nodes. It can simulate scenarios where multi-hop routing is undesirable.

∗ Mac IFcontrol [34] : Defines the MAC layer for UWB, functions of transmission, queue management, control packets and listening mode etc.

∗∗ Interference-phy [34] : defines possible states (reception, transmission, listen or hang) and manages the time to listen and reception etc.

Parameters of Simulations

In order to evaluate the quality of service, the simulations treat a comparative metric subject to two different multicast protocols AODV and DSR [41], [42] for ZigBee technology and protocol NOAH for UWB parameters as mentioned below. The figure (Figure 3-5) list an example of architecture adopted, using node as wireless multimedia sensors and a collector of data "C" (nodeo in NAM Visualisator). The simulation results are drawn from the files "tr" generated and analyzed by file "awk". The figure (Figure 3-6) summarizes the simulation parameters used for the ZigBee and UWB technologies :

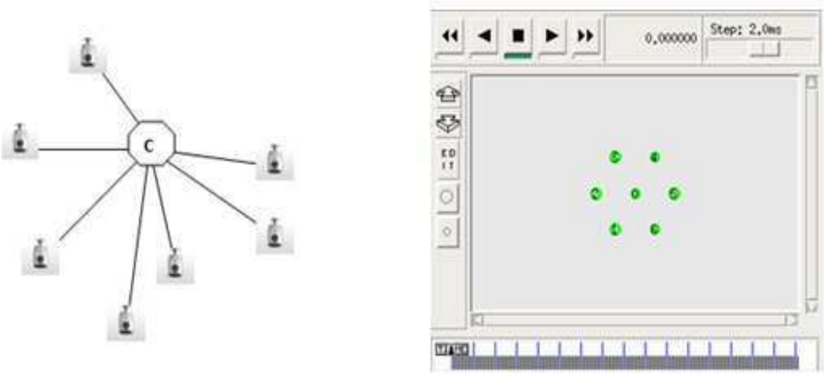
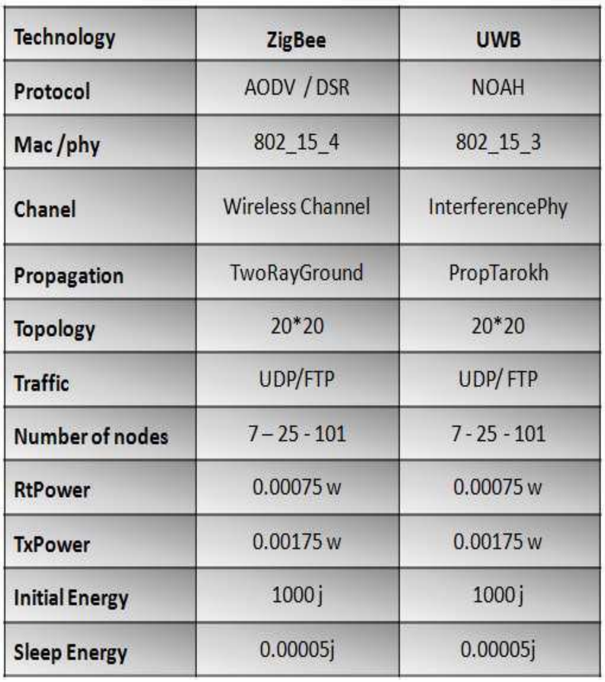


FIGURE 3.5 – *Frequency Spectrum in UWB technology*



Technology	ZigBee	UWB
Protocol	AODV / DSR	NOAH
Mac /phy	802_15_4	802_15_3
Chanel	Wireless Channel	InterferencePhy
Propagation	TwoRayGround	PropTarokh
Topology	20*20	20*20
Traffic	UDP/FTP	UDP/ FTP
Number of nodes	7 – 25 - 101	7 - 25 - 101
RtPower	0.00075 w	0.00075 w
TxPower	0.00175 w	0.00175 w
Initial Energy	1000 j	1000 j
Sleep Energy	0.00005j	0.00005j

FIGURE 3.6 – *Parameters used in ZigBee and UWB simulations*

RESUALTS AND DISCUSSION

The following figures illustrate a comparison based on the results of previous simulations show the benefit of UWB in the delivery of a high rate of packets (Figure 3-7 and Figure 3-8) compared to ZigBee (Figure 3-9) with a wide bandwidth (Figure 3-10) and a delay (Figure 3-11) start to finish while consuming a minimum of Energy (Figure 2-12) for less dense networks :

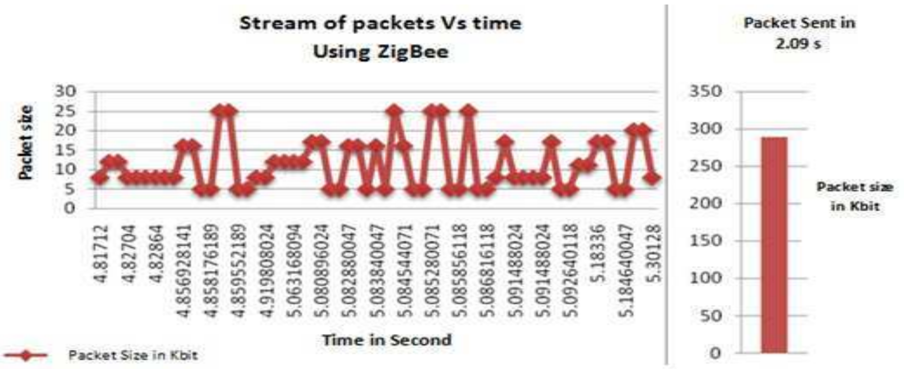


FIGURE 3.7 – *Stream Packets Vs Time Using ZigBee*

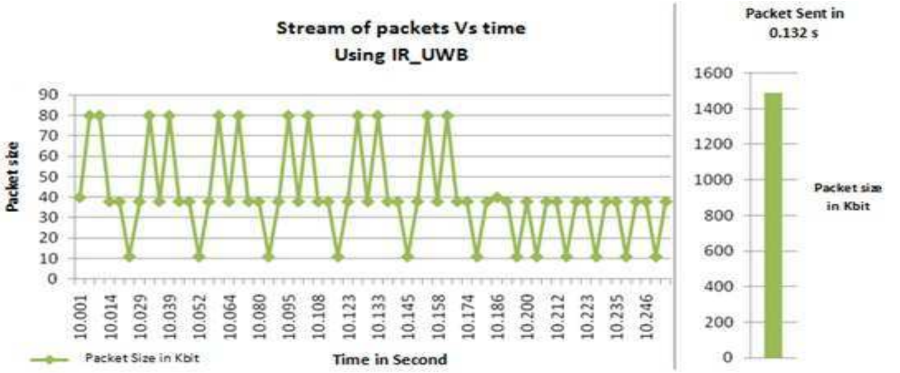


FIGURE 3.8 – *Stream Packets Vs Time Using impulse radion UWB*

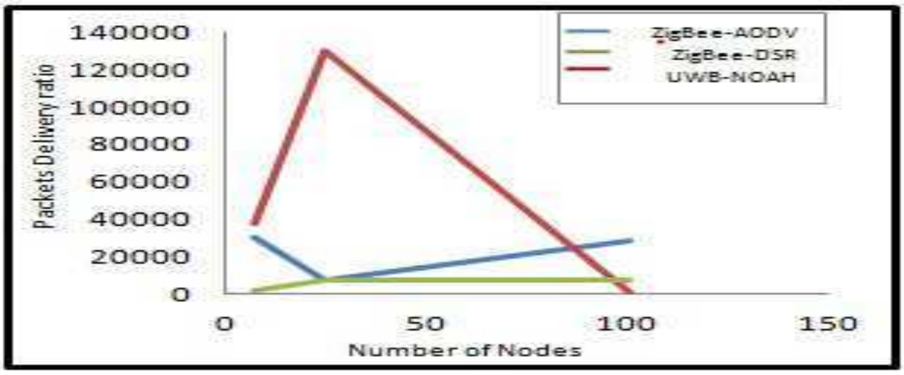


FIGURE 3.9 – *Packets Delivery Ratio*

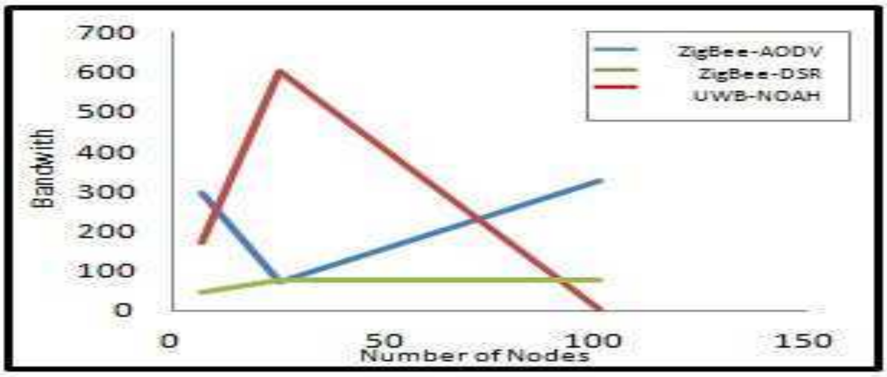


FIGURE 3.10 – *Bandwidth*

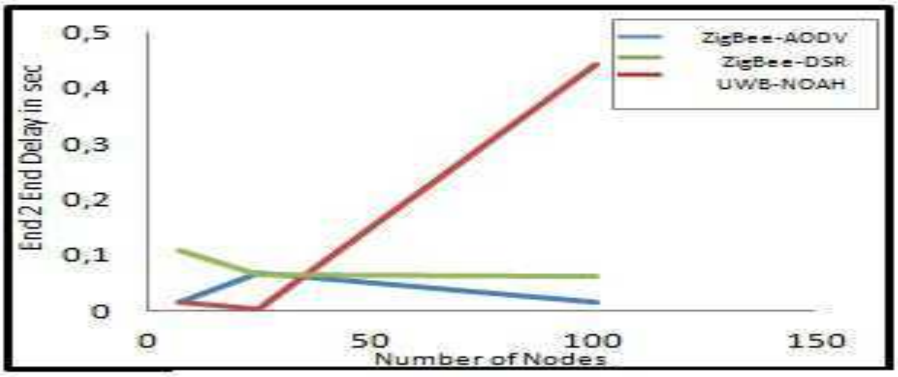


FIGURE 3.11 – *End to End Delay*

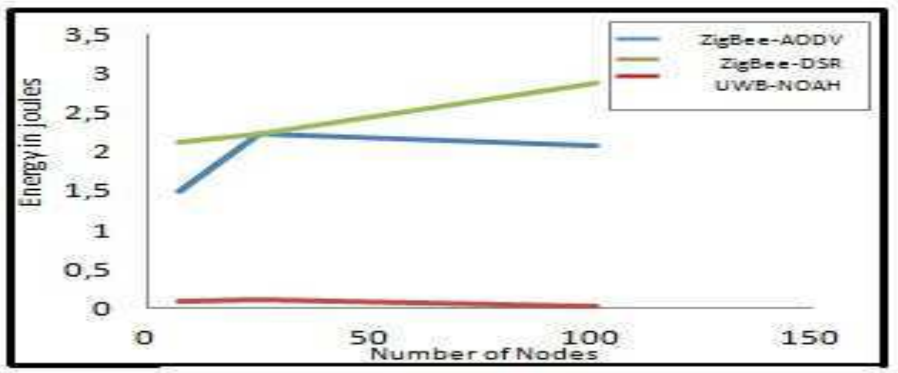


FIGURE 3.12 – *Energy Consumption*

With the simulation parameters mentioned, the UWB technology offered a considerable quality of service in term of end to end delay, packet delivery ratio, bandwith and energy for a sensor network with less density of network when sending media streams. Indeed, this technology has gives a good results compared to those of the ZigBee technology especially for a network average of 25 nodes which promotes greater use of these sensors for the transfer of multimedia data.

3.1.8 CONCLUSION

This work has explored a survey on the Physical and Mac functionalities of sensor by camparing UWB and ZigBee standards. In order to compare their performance in wireless multimedia sensor network application, we have presented in this part a quality of service of standards mentionned above, using the popular metrics as a network performance tools. In particular, those metrics, already presented, were evaluated to study the quality of communication of multimedia data under the network simulator NS2.

Furthermore, we found that the performance tests conducted on the consumption of energy, packet delivery ratio, bandwidth and end-to-end delay, have shown that the UWB technology responds well performance criteria desired. Indeed, the ultra wide band

(UWB) technology function has the potential to enable low-power consumption, high data rate communications, characteristics that make it an ideal choice for WMSNs appliacations and indoor area.

The next section describes the localization functionality of sensor compared to TDOA localization technique. The presented method is based on the energy consumption to locate approximatively the destination.

ABSTRACT

"The localization function is presented here by developing a new technique of localization for an application in the transport domain. This function, compared to classical techniques like TDOA, is also adopted for energy optimization far of the use of the GPS"

3.2 New Technique of Wireless Sensor Networks Localization Based on Energy consumption

3.2.1 INTRODUCTION

A Wireless Sensor Network (WSN) is formed by hundreds of small, low-cost nodes which have limitations in memory, energy, and processing capacity. In spite of existing of several functionalities, to locate each node [43], is one of the main functions problems. Recent advances in wireless communications and electronics have enabled the development of low-cost, low-power and multifunctional sensors that are small in size and communicate in short distances. Cheap, smart sensors, networked through wireless links and deployed in large numbers, provide unprecedented opportunities for monitoring and controlling homes, cities, and the environment. In addition, networked sensors have a broad spectrum of applications in the defense area, generating new capabilities for reconnaissance and surveillance as well as other tactical applications. Self-localization capability is a highly desirable characteristic of wireless sensor networks. In environmental monitoring applications such as bush fire surveillance, water quality monitoring and precision agriculture, the measurement data are meaningless without knowing the location from where the data are obtained. Moreover, location estimation may enable a myriad of applications such as inventory management, transport, intrusion detection, road traffic monitoring, health monitoring, reconnaissance and surveillance.

3.2.2 LOCALIZATION AND MEASUREMENT TECHNIQUES

Localization Techniques

Advances in micro-electro-mechanical systems have triggered an enormous interest in wireless sensor networks (WSN). WSN are formed by large numbers of densely deployed nodes enabled with sensing and actuating capabilities. These nodes have very limited processing and memory capabilities, limited energy resources and it is envisioned that they will be mass produced, to reduce costs. Several challenging problems exist in wireless sensor networks. Among these is how to obtain location information for sensor nodes and events present in the network. From this perspective, we categorize the localization problem as : node localization, target localization and location service. Node localization is the process of determining the coordinates of the sensor nodes in the WSN. Target localization is the process of obtaining the coordinates of an event or a target present in the sensor network. The location of a target can be obtained either passively (the nodes sense the target) or actively, when the target cooperates and communicates with the sensor network.Node localization is a complicated and important problem for wireless sensor networks (WSN). The aspects of this problem that have challenged the research community can be summarized as follows :

Assumptions - The node localization problem remains a difficult challenge to be solved practically. To make the problem practically tractable, its complexity had to be reduced, by making simplifying assumptions. As a result, many localization schemes proposed solutions that are based on assumptions that do not always hold or are not practical. Examples of such assumptions are : circular radio range, symmetric radio connectivity, additional hardware (e.g., ultrasonic), lack of obstructions, lack of line-of-sight, no multipath and flat terrain.

Localization Protocol Design - The problem of localization in WSN is further complicated by the large number of parameters that need to be considered when designing a localization system for a particular WSN deployment [44]. Among these parameters are : the deployment method for the sensor network ; the existence of a line-of-sight between sensor nodes and a remote, central point ; the time required by the localization scheme ; the presence of reference points (anchors) in the network, and the density ; the cost for localization, represented by additional hardware (form factor) and energy expenditure (messages exchanged or time necessary for localization).

Sensor network localization algorithms estimate the locations of sensors with initially unknown location information by using knowledge of the absolute positions of a few sensors and inter-sensor measurements such as distance and bearing measurements. Sensors with known location information are called anchors and their locations can be obtained by using a global positioning system (GPS), or by installing anchors at points with known coordinates. In applications requiring a global coordinate system, these anchors will determine the location of the sensor network in the global coordinate system. In applications where a local coordinate system suffices (e.g., smart homes), these anchors define the local coordinate system to which all other sensors are referred. Because of constraints on the cost and size of sensors, energy consumption, implementation environment (e.g., GPS is not accessible in some environments) and the deployment of sensors (e.g., sensor nodes may be randomly scattered in the region), most sensors do not know their locations. These sensors with unknown location information are called non-anchor nodes and their coordinates will be estimated by the sensor network localization algorithm.

Measurement techniques

Measurement techniques in WSN localization can be broadly classified into three categories : AOA measurements [45], distance related measurements and RSS [43] profiling techniques.

– Angle-of-arrival measurements

The angle-of-arrival measurement techniques can be further divided into two subclasses : those making use of the receiver antennaâs amplitude response and those making use of the receiver antennaâs phase response. Beam forming is the name given to the use of anisotropy in the reception pattern of an antenna, and it is the basis of one category of AOA measurement techniques [46] and [47]. The measurement unit can be of small size in comparison with the wavelength of the signals. One can imagine that the beam of the receiver antenna is rotated electronically or mechanically, and the direction corresponding to the maximum signal strength is taken as the direction of the transmitter. Relevant parameters are the sensitivity of the receiver and the beam width. A technical problem to be faced and overcome arises when the transmitted signal has a varying signal strength. The receiver cannot differentiate the signal strength variation due to the varying amplitude of the transmitted signal and the signal strength variation caused by the anisotropy in the reception pattern. One approach to dealing with the problem is to use a second non-rotating and omnidirectional antenna at the receiver. By normalizing the signal strength received by the rotating anisotropic antenna with respect to the signal strength received by the non-rotating omnidirectional antenna, the impact of varying signal strength can be largely removed. The figure (Figure 3-13) shows an antenna array of N antenna elements. The adjacent antenna elements are separated by a uniform distance d [48]. The distance between a transmitter far away from the antenna array and the i^{th} antenna element can be approximated by :

$$R_i = R_0 - idcos\theta \qquad (1)$$

where $R0$ is the distance between the transmitter and the 0^{th} antenna element and θ is the bearing of the transmitter with respect to the antenna array.

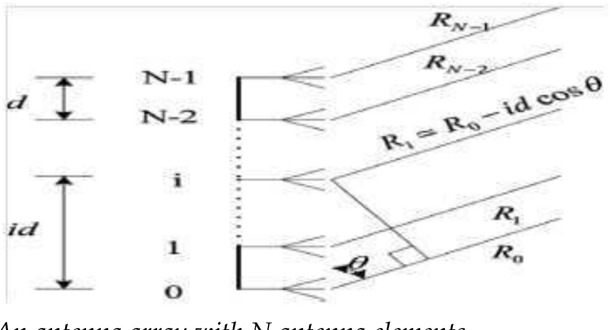


FIGURE 3.13 – *An antenna array with N antenna elements.*

– Distance related measurements

Distance related measurements include propagation time based measurements, i.e., one-way propagation time measurements, roundtrip propagation time measurements and time-difference-of-arrival (TDOA) measurements. Another interesting technique measuring distance, which does not fall into the above categories,

is the lighthouse approach shown in [49]. In the following paragraphs we provide further details of these techniques.
○ One-way propagation time and roundtrip propagation time measurements
○One-way propagation time and roundtrip propagation time measurements are also generally known as time-of-arrival measurements. Distances between neighboring sensors can be estimated from these propagation time measurements. One-way propagation time measurements measure the difference between the sending time of a signal at the transmitter and the receiving time of the signal at the receiver. It requires the local time at the transmitter and the local time at the receiver to be accurately synchronized.
○ Time-difference-of-arrival measurements
There is a category of localization algorithms utilizing TDOA measurements [50] of the transmitter's signal at a number of receivers with known location formation to estimate the location of the transmitter. Figure 3-14 shows a TDOA localization scenario with a group of four receivers at locations r_1, r_2, r_3, r_4 and a transmitter at rt. The TDOA between a pair of receivers i and j is given by :

$$\Delta t_{ij} = t_i - t_j = \frac{1}{c}(|| \, r_i - r_t \, || - || \, r_j - r_t \, ||); i \neq j; \qquad (2)$$

where ti and tj are the time when a signal is received at receivers i and j, respectively, c is the propagation speed of the signal, and || denotes the Euclidean norm. Measuring the TDOA of a signal at two receivers at separate locations is a relatively mature field [51].

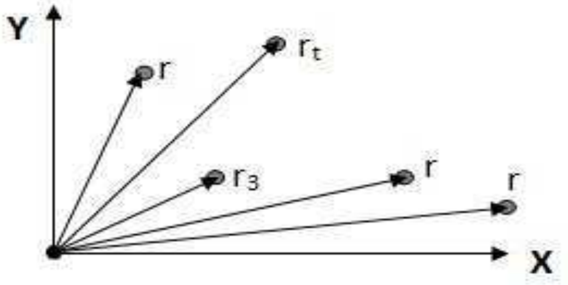


FIGURE 3.14 – *Localization using time-difference-of-arrival measurements.*

In summary, a number of measurement techniques are available for WSN localization. Which measurement technique to use for location estimation will depend on the specific application. Typically, localization algorithms based on AOA and propagation time measurements are able to achieve with acceptable accuracy than localization algorithms based on GPS measurements which consume more energy.

Comparison Techniques

One of the most appealing problems to be solved by localization techniques is how to provide an anytime, anywhere, fine-grained, and reliable localization system to be used by transport vehicles for critical safety and emergency applications. An anytime requirement means that the localization system must be free of delays when computing the current positions of the vehicles. This requirement is critical, since the high mobility of vehicles means that slightly outdated position information cannot be used and could even be dangerous. To be available anywhere is also a challenge in localization system. It means that the localization system cannot rely only on satellite infrastructure, since it would then not work in environments without direct visibility to satellites. Also, it cannot rely only on local infrastructured localization techniques, since it would not be available in places without this infrastructure. Finally, a fine-grained localization system ensures a low localization error for vehicles, which enables most critical applications to have some degree of confidence. A lot of researches focus on static sensor networks. Relatively less is known about localization in mobile sensor networks, and very few algorithms work in situations where the sensors may be static or mobile.

3.2.3 CONTRIBUTION AND PROPOSED METHOD

We based our work on [5] using the energy model consumption sending and receiving one byte of data from node i to node j over a distance d meters, and we consider that the energy consumption costs :

$$e^s_{ij} = c_1 + c_2 d^2_{ij} \qquad (3)$$

$$e^r_{ji} = c_1 \qquad (4)$$

We consider here that d_{ij} as the variable needed to localize node destination, and by knowing the energy consumed when sending a data from node i to node j and using the angle of arrival α (c_1, c_2, e_{ij} and e_{ji} are defined in [5]).
Using the equation (3) we can easily deduce de distance d separate the two nodes :

$$d_{ij} = \sqrt{\mid \frac{e^s_{ij} - c_1}{c_2} \mid} \qquad (5)$$

by calculating the distance d we place the node destination j on the circle where the node i represent his centre. The angle of arrival serves for locating the node j on the segment S and reducing the probability of positioning the node on all area of the circle. Considering the segment S proximately similar to line, and using the Euclidian distance [52] d between node I and j at the instant t we denote :

$$d_{ij}(t) = \sqrt{(X_i - X_j)^2 + (Y_i - Y_j)^2} \qquad (6)$$

$$S \cong 2.d_{ij}(t).sin(\frac{\alpha}{2})$$

$$= 2\sqrt{(X_i - X_j)^2 + (Y_i - Y_j)^2}.sin(\frac{\alpha}{2}) \qquad (7)$$

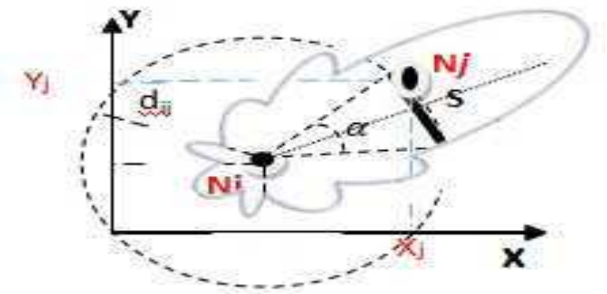
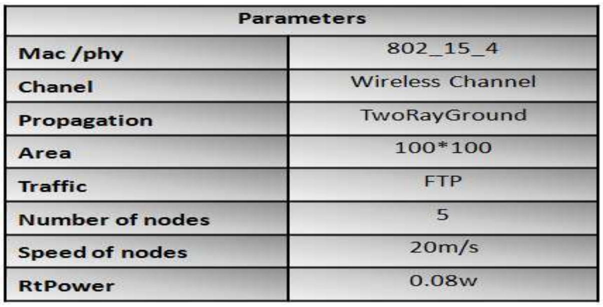


FIGURE 3.15 – *Representation of the proposed method*

This method (Figure 3-15) of localization, based on two techniques (angle of directional antenna and the energy of transmission), can sufficiently locate node with reduced probability. The rate and magnitude of this probability can be neglected specially for vehicles and transport applications where the node has a considerable volume compared to the segment S. Unlike the others techniques, the method mentioned reduce the energy consumption of nodes used aggressively in GPS techniques.

3.2.4 SIMULATION AND RESULTS

Using the popular tool NS2, we proceed to analyze the performance of the TDOA, and the proposed method using the standard IEEE.802.15 (ZigBee) really implemented on actual sensors using 5 mobile nodes with a speed fixed on 20 m/s on and simulation over 100 seconds (in the mobile context).We used the model Random way Point model in the area of $100m^2$ (Table → Figure 3-16) and the directional Antenna.



Parameters	
Mac /phy	802_15_4
Chanel	Wireless Channel
Propagation	TwoRayGround
Area	100*100
Traffic	FTP
Number of nodes	5
Speed of nodes	20m/s
RtPower	0.08w

FIGURE 3.16 – *Parameters used in simulations*

We proceed to the variation distance between node source and the four nodes destination used in the script of simulation, by function of time when nodes moves at the speed $20m/s$. The figure (Figure 3-17) illustrate the comparison between the proposed method, based on the energy consumed by sending 512 Kbyte of packets and calculated the distance d between the nodes i and j using the formula based on [5], the TDOA technique based on equation (2), and the NS2-mesurement using the Euclidian distance mentioned on the equation (6). By using the distance calculated on our method, we can deduce easily the angle α from the equation (7) and we can see that when α decrease (Figure 3-18) we obtain

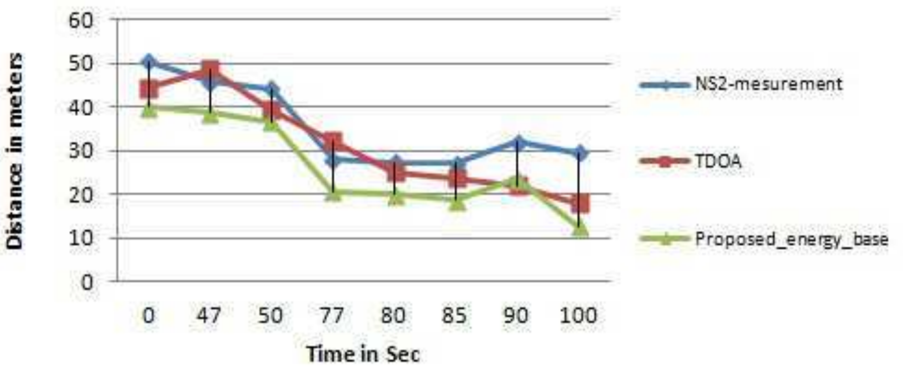


FIGURE 3.17 – *Comparison of the proposed method, TDOA and NS2 measurements*

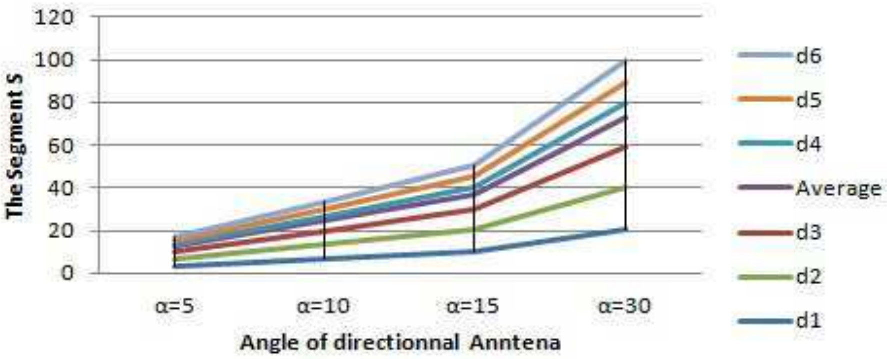


FIGURE 3.18 – *Probability of positioning destination node on the segment measured by the angle α and d_i ($i = 0 \rightarrow 6$) are the distance calculated by our method.*

a small segment of S and by contrast this distance increase when α is high. Because of this, our method gives a good results when α is small. Huns we reduce the segment S and the probability to localize the destination in this section which can proportional to the dimensions and size of the mobile or vehicle were are implemented the sensors.

3.2.5 CONCLUSION

We presented in this work a measurement technique for the localization function, applied to sensor network in transport domain which knows a high mobility. This technique is based on the energy consumption of sensor node and the angle α of transmission of a directional antenna, and compared to TDOA technique .We recommend, in our method, to use a small angle of the antenna in order to localize approximately and with high probability nodes implemented in applications like transport and vehicles known by considerable dimensions and size. For the future work, we can think how combining AOA, TDOA and the presented method using the UWB [53] standards for localization under NS2.

The security function is an important area that need, in the communication process, to locate a sender of message or in some cases to position a malicious node. Because of this, the security and localization functions are strongly related.

The next section will be focused on the security scheme in the WSN field taking into consideration the energy consumption as a major concern. This field is strongly related to the localization function, because the job security still need to locate the source and destination nodes malicious they are or not.

ABSTRACT

"The security challenger is a ubiquitous problem of wireless communication. In the following section, we propose a new architecture based on agent approach to surpass the use of key management and economize the energy of processing."

3.3 Agent Security for Wireless Sensor Networks

3.3.1 INTRODUCTION

A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor (Figure 3-19). The Security scheme in listed in several works and surveys [84] in literature are many.

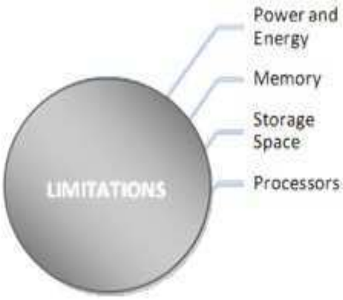


Figure 3.19 – *Limited resources in wireless sensors*

3.3.2 WIRELESS SENSOR NETWORKS ATTACK

In order to better understand the security systems that must be able to prevent, counter, detect, and respond to, this section provides a brief overview of sensor network attacks. We note that an attacker may be equipped with either malicious nodes or more sophisticated computing machinery like a laptop or signal generator and signal processing equipment, may be an inside attacker or an outside attacker, or may be a passive or an active attacker. Most trust models assume that the base station is trustworthy as long as it is available.

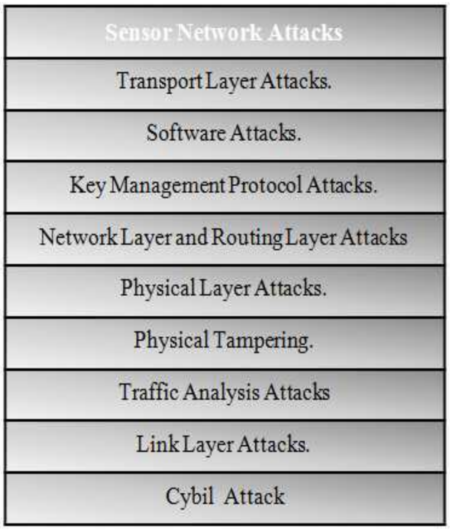
Given the great value of the base station one can argue that it is more likely to be attacked than a sensor especially since it is also more likely to have network connectivity through a wired or wireless gateway.

Sensor networks are susceptible to attacks starting from the physical layer and going all the way up the stack to the application layer. From the literature [54],[55] the popular sensor network attacks can be classified like mentioned on Table → Figure 3-20.

3.3.3 Key MANAGEMENT in WIRELESS SENSOR Networks

In WSNs, most security protocols are based on the cryptographic operations using keys. Key management problem can be de-composed into four phases. The first is the key distribution or pre-distribution phase where secret keys are distributed to sensor nodes for use with the security mechanisms (i.e., confidentiality, authentication and integrity). Sensor nodes have a limited life time, and they are subject to variety of attacks including node capture. New sensor nodes may be deployed and security materials on existing ones may need to be updated. The key management solutions can be classified and evaluated by considering following properties [56] :

• Underlying network architecture. In distributed WSN, there is no resource rich member, and sensor nodes have equivalent capabilities. In hierarchical WSN, there are one or more resource rich central stations, and there is a hierarchy among the sensor nodes based on their capabilities.



Sensor Network Attacks
Transport Layer Attacks.
Software Attacks.
Key Management Protocol Attacks.
Network Layer and Routing Layer Attacks
Physical Layer Attacks.
Physical Tampering.
Traffic Analysis Attacks
Link Layer Attacks.
Cybil Attack

Figure 3.20 – *Popular Attacks in WSN*

• Communication style : A secure unicast communication between a pair of neighboring nodes requires a pair-wise key shared between them. A reusable pair-wise key is used to secure the unicast communication between more than one pairs of neighboring nodes. Disadvantage is that more than one links are compromised when a reusable pair-wise key is compromised.

• Key pre-distribution method : Keys and keying materials are distributed to sensor nodes based on a probabilistic, deterministic or hybrid algorithm.

• Key discovery and establishment method : A set of solutions predistribute a list of keys, called a key-chain, to each sensor node, and a pair or a group of sensor nodes can secure their communication if they have a key in common.

Key Management in Hierarchical Wireless Sensor Networks

A Hierarchical WSN (HWSN) includes one or more computationally robust base stations. Sensor nodes are deployed in one or two-hop neighborhood around base stations or resource rich sensor nodes (called cluster heads) as illustrated in Figure 3-21. Base stations are usually assumed to be trusted and used as the key distribution centers. In a HWSN, pair-wise, group-wise and network-wise keys are required to secure unicast, multicast and broadcast types of communications among sensor nodes, cluster heads and base stations.

- Pair-wise Key Management

In a Hierarchical WSN, base station to sensor node, or sensor node to base station unicast communications are secured by using dedicated pair-wise keys. A straightforward approach is to pre-distribute a dedicated pair-wise key to each sensor node so that each base station shares a dedicated pair-wise key with each sensor node deployed within its close vicinity.

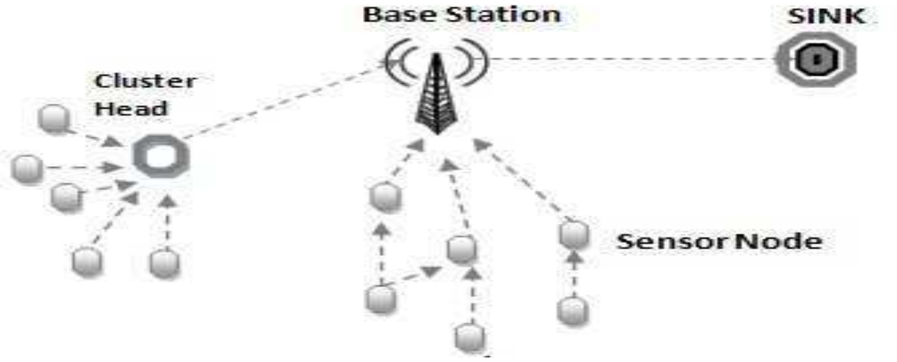


Figure 3.21 – *Illustration of hierarchical WSN*

- Group-wise Key Management

A set of solutions propose to use costly asymmetric cryptography based key management solution. In a HWSN where each base station shares a dedicated pair-wise key with each sensor node deployed within its close vicinity, the base station can intermediate group-wise key establishment. Localized encryption and authentication protocol (LEAP) proposes a group-wise key generation scheme which follows LEAP pair-wise key establishment phase. Assume that sensor node Su wants to establish.

- Network-wise Key Management

Network-wise keys are used to secure base station to sensor node broadcast trafic in HWSN. A straightforward but insecure approach is to pre-distribute a single network-wise key to all sensor nodes. Multi-tiered security solution [57] proposes to protect data items to a degree consistent with their value. In key setup phase, each sensor node receives a list of m master keys. Selected master key is named as active master key. RC6 is used as encryption algorithm.

Key Management in Distributed Wireless Sensor Networks

In a distributed WSN (Figure 3-22), sensor nodes use dedicated pair-wise, reusable pair-wise and group-wise keys to secure their communication, or use keying materials to generate these keys. A part of key management solutions, called key pre-distribution schemes, assign a list of keys, called a key-chain, to each sensor node a priori to the deployment. Others, called key generation schemes, assign keying materials to each node by using which a pair or a group of nodes can generate keys to secure their communication. Solutions to distribute keys and keying materials can be classified as probabilistic [58], deterministic [59], and hybrid [60]. In probabilistic solutions, keys and keying materials are randomly selected from a pool. In deterministic solutions, deterministic processes are used to design the pool and to decide which keys and keying materials to assign to each sensor node so that the key connectivity is increased. Finally, hybrid solutions use probabilistic approaches along with deterministic algorithms to improve the scalability and key resilience.

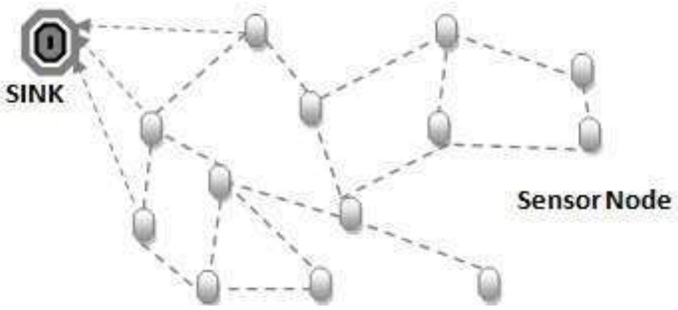


Figure 3.22 – *Illustration of distributed WSN*

3.3.4 THE AGENT SECURITY FOR WSN

Agent Approach

The agent [55], [61] approach discussed here involves developing a platform Multi agent system ensuring the security function of sensors. Indeed, this approach resumed in the ability of agent to manage a set of sensors of its sensing field, taking into consideration a range of sensors, and detects physical intrusion or malicious nodes. These sensors programmed with agents are able to communicate with other sensors. An information report is delivered to the base station (sink) revealing the state of security level of sensors in order to act at time for any outside intrusion. Figure 3-23 illustrates the key idea of our approach. In this case, the nodes may belong to the same level; the agent ensures the collection in its field of four nodes and returns any anomaly or intrusion to the sink.

Multi Agent Platforms

The pilot implementation of those agents (Sensors) is based on TinyOS component model. TinyOS components are specified using NesC programming language that has a C-like syntax, but supports the TinyOS concurrency model. The main information programmed in modules (to be sensed) is related to movement, exceeding number of sensor belonging to the same fields. Our proposal Multi agent platform, compared to work in [62], is a code containing some data and a control program interpretable on the agent platform. Each platform resides at one sensor and consists of the following modules (Figure 3-24) :

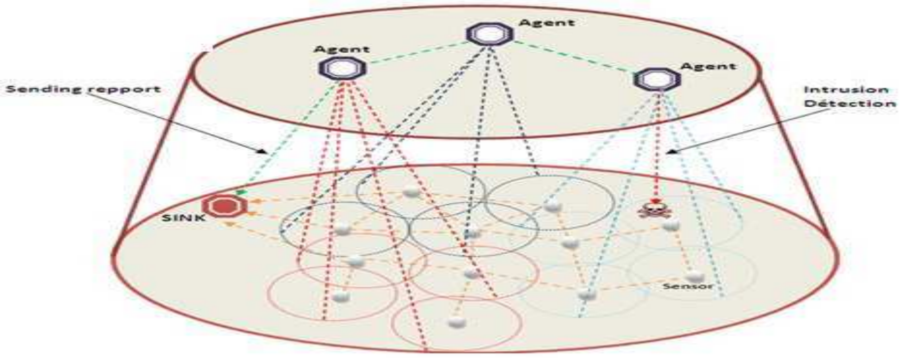


FIGURE 3.23 – *Illustration of intrusion detection approach based*

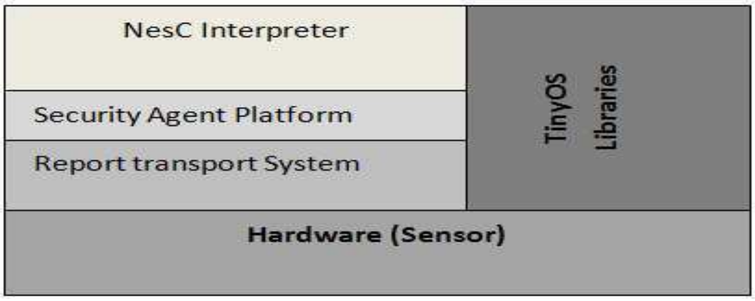


FIGURE 3.24 – *Hierarchy of Platform and agents*

• NesC interpreter : interpreter of the NesC language that manipulates with agent program and possibly interacts with other modules.

• Security Agent Platform : services provided to the agents. It includes computation (a set of functions), interpreter control, when an event or intrusion is received, and it also includes some platform variables that are accessible to particular agents.

• Report transport system : responsible of transmission and reporting the security state to the sink.

The Approach Advantages

In addition to the security of this architecture, this approach minimizes the energy consumption, needed when processing to distribute and verify keys, compared to other solutions based on cryptography and key management. . Indeed, in this approach, sensors are required to sense with no treatment or management of keys. Therefore, the energy savings can be a result from the implementation of such a platform.

3.3.5 CONCLUSION

We outline the usage of key management techniques for securing wireless sensor network. In add we present a security function based agent approach, which is a part of a program code. The computational power for security tasks of a cryptographic key seems greedy on energy whereas the proposal platform reduce this consumption faraway of use the key management.

The routing is a solution key in the wireless networks. Because of this, the next section lists a routing function based on mathematical approach and proposing a new algorithm for route discovery mechanism in Ad hoc networks applied in WSN.

ABSTRACT

"Routing is a perfect key and solution for energy economization. For this optimal algorithms play an important role in the optimization of the processing informations and communication in the sensor components. In fact, the section below explains a new algorithm for the optimization of energy consumption."

3.4 New Algorithm "DRREQ" Applied in AODV Route Discovery Mechanism for Energy Optimization in Mobile Ad hoc Networks

3.4.1 INTRODUCTION

Optimizing the energy consumption becomes more and more critical. Due to this, several studies focuses their works on energy, especially in wireless applications like sensor networks which present a challenge in this area of search. In this context, the processing of data sent by the sensors consumes also a considerable energy mainly in ad hoc networks. In these networks, route discovery mechanisms used in protocols like AODV and DSR consume a huge energy when broadcasting the "Hello" message. In traditional on-demand routing algorithms such as AODV and DSR, a node that needs to discover a route to a particular destination, broadcasts a route request control packet (RREQ) to its immediate neighbors.

Each neighboring node blindly rebroadcast the received RREQ packet until a route is established. This method of route discovery is referred to as simple flooding. Since every node rebroadcast the RREQ packet the first time it is received and assuming that the destination node is reached, the possible number of rebroadcasts is around N-2, where N is the total of number of network nodes. This method of broadcasting can potentially lead to excessive redundant retransmissions in congested networks and hence causing high energy consumption

3.4.2 RELATED WORKS

A growing interest focused on energy conservation in wireless communications. Hence, several works [63], [64] are done with techniques that optimize algorithm in order to decrease processing. The process of route discovery is one of axes used to improve the communication efficiency by attacking the limitations like the impact of flooding the provoke redundancy, contention and collision. Another works [65] based on MMBCR (Min-Max Battery Cost) Routing, uses periodic route discovery to get more updated information about the routes. In this method, periodically the route discovery process is done. If there are any changes in the route, the route information is updated. Because of this method, different routes are used for the transmission of data packets and periodic shifting between the routes which avoids the over usage of nodes and node exhaustion leading to the decrease of the energy consumption and the lifetime of the network. Several techniques use the link adaptation. Authors of [66] present the protocol VON (velocities of nodes) using the nodes which have slow speed forward RREQ messages while the nodes which have high speed do not. Aminu &. al in [67] proposes a new probabilistic counter-based method that can significantly reduce the number of RREQ packets transmitted during route discovery operation.

3.4.3 THE PROBABILISTIC APPROACH

The probabilistic broadcast has been recommended [68], [69] and [83] as one of the solutions to mitigate the broadcast storm problem associated with the simple flooding method. In conventional probabilistic broadcast methods, each mobile node rebroadcasts a received packet once based on a predetermined fixed-value forwarding probability. The probabilistic [69] and [70] schemes do not require the global topological information of the network in order to make rebroadcast decisions. Based on [68] the probabilistic concept used here, is focused on the number of neighbors (1) and the directional antenna of nodes which is equipped by rotator motor able to change direction. In the fixed probabilistic route discovery, the number of possible broadcasts of an RREQ packet is $p * (N - 2)$ [69].

For N nodes in the network, let Ni the number of neighbors at a node x_i at a particular time instant, the average number of neighbors "n_a" at a node in the network at that time instant is defined by the relation [69] :

$$n_a = \frac{\sum_{i=1}^{n} N_i}{N} \qquad (1)$$

3.4.4 THE DICHOTOMIC APPROACH

Applied in our study, the concept of Dichotomic algorithm focuses on finding the target nodes following a request RREQ (Algorithm1). In principle, it consists of a probabilistic search for RREP (Route REPlay) from destination node, in the right field, before the left one, of the node by minimizing the number of queries initiated by the node. This done, the node economize his energy for this set of queries.

Algorithm1 :

```
If (no route exists)
{
Check request buffer for request already sent
If(no request sent)
Create a RREQ packet
save in buffer
Broadcast RREQ in right field
If( no RRP)
Broadcast RREQ in left field
}
```

In the algorithm2, let $\theta_0$the angle of antenna, and the time needed for waiting for a RREP.

Algorithm2 :

```
INPUT:
        upon receiving RREQ packet at node $x$
         $\theta_r$ and $\theta_l$ are respectively the angle \
        of antenna at right research and left research
        Get number of neighbours $N_x$ at node $x$
        Compute the average number of neighbours $n_a$
BEGIN
        if the RREQ is received for the first time
        toto:
        if $N_x \leq n_a$
        // research on right field
        $\theta_r = \theta_0 + \pi$
         the node x rebroadcast RREQ packet
         wait $t_0$ seconds for RREP from neighbors
        if RREP received END.//stop broadcasting in the left
        else
        // research on left field
        $\theta_l = \theta_0 - \pi$
        the node x rebroadcast RREQ packet
        wait $t_0$ seconds for RREP from neighbors
        if RREP received END. // stop broadcasting
         else
        goto toto
END.
```

3.4.5 DISCUSSION

In this case of study, we consider a fix topology of N nodes. The main idea of our work is to limit the number of broadcast in RREQ mechanism. Indeed, the node limits his research at first time in the right area (or the left by probabilistic approach of presence of destination based on routing table), thus the node can save until the half of energy when finding the destination. At least this technique can be used to localize the destinations at right or left (Figure 3-25) then with increasing the probability that can help to the choice of the location field and consequently the energy can be economized considerably for the posterior requests.

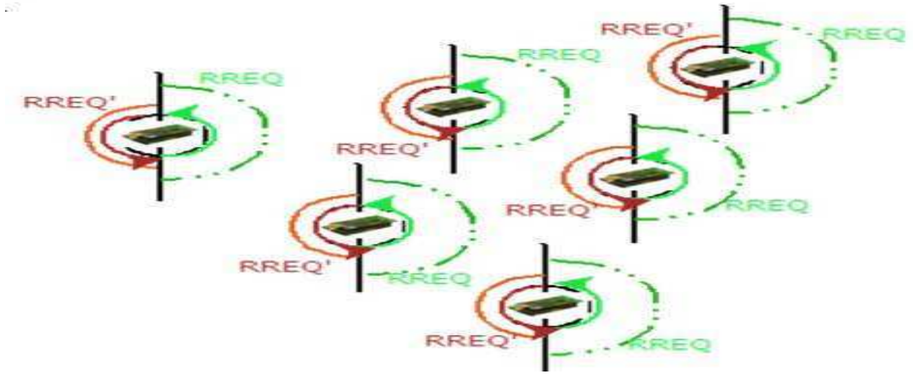


Figure 3.25 – *Dichotomic Approach for RREQ Mechanism*

3.4.6 SIMULATION AND RESULTS

In this section, we evaluate and compare the performance between DRREQ and RREQ using AODV [71] protocol. The simulation was done by the NS2 simulator using the version ns2.29. we based our work on various simulations in mobile context of nodes (20m/s) and by varying the number of nodes with 10j of initial energy for each one (Figure 3-26). We evaluate two metrics ; energy (Figure 3-27) and the average end-to-end delay (Figure 3-28) that can be affected by the performance of the route discovery mechanism.

Constant Bit Rate (CBR) traffic is used with 10 traffic instances with a rate of 40.96kbits/s. The packet size is 512 bytes and the interval is 0.1s. FTP traffic is used to simulate TCP performance. The packet size is 1500 bytes. For TCP, only 1 ftp traffic is simulated and TCP-Reno is adopted. The results of 10 different scenarios are averaged.

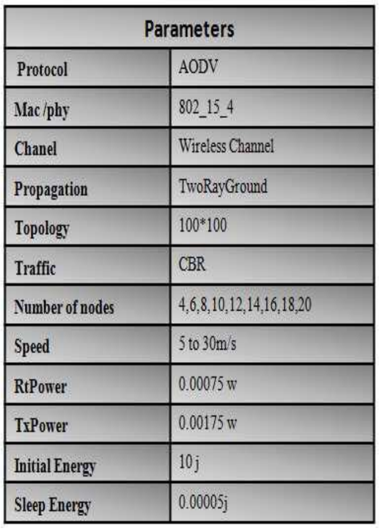
Figure 3-27 indicates that DRREQ consumes less energy compared to the traditional RREQ. This is due to the fact that in DRREQ, a packet will be broadcasted and forwarded only on the right (or left) area with half probability to find destination, which decrease the energy consumption to broadcast messages for route discovery mechanism.

Figure 3-28 shows that DRREQ obtains less time to reach a destination which is due to high probability to discover destination quickly. Thus DRREQ achieves an obvious improvement by reducing route energy consumption with high performance of end to end delay which is related to energy and distance.

On the other hand, Figure 3-29 and Figure 3-30 shows an improvement of energy consumption when varying at first the speed of 10 nodes from 5m/s to 30m/s, then by varying the pause time from 10ms to 60ms. In fact, the energy consumption decrease when the speed is less then 20m/s especially with a good result for DRREQ than RREQ, but it increase more with this speed. Hence, we conclude that the dichotomic approach used in this mechanism give high performance by separating two areas for requesting destinations by broadcasting fewer messages and minimize the treatments. The same results are proved by varying the pause time, where DRREQ performs well, in these simulations, by using less energy for high values of pause time which coincide with low mobility context.

3.4.7 CONCLUSION

In this section, we presented a new technique of RREQ which combine two mathematical approaches ; Dichotomy and Probability, used to minimize the energy consumption in the RREQ mechanism frequently used in popular protocols like AODV and



Parameters	
Protocol	AODV
Mac/phy	802_15_4
Chanel	Wireless Channel
Propagation	TwoRayGround
Topology	100*100
Traffic	CBR
Number of nodes	4,6,8,10,12,14,16,18,20
Speed	5 to 30m/s
RtPower	0.00075 w
TxPower	0.00175 w
Initial Energy	10 j
Sleep Energy	0.00005j

FIGURE 3.26 – *Parameters of Simulation*

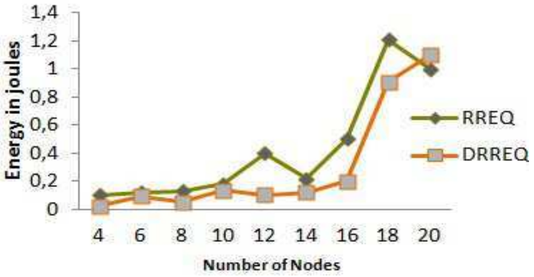


FIGURE 3.27 – *Energy Consumption*

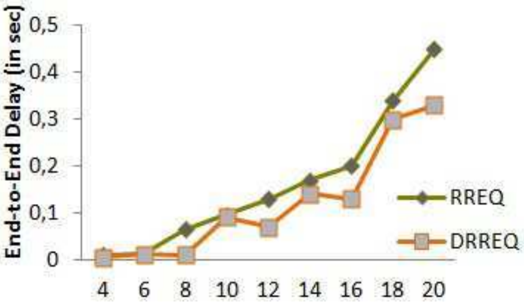


FIGURE 3.28 – *End-to-End delay*

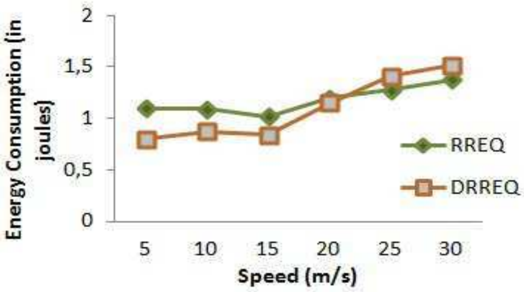


FIGURE 3.29 – *Energy consumption vs speed*

DSR in Wireless Ad hoc Network. After modification in the RREQ in AODV under NS2, the results shows an improvement in saving

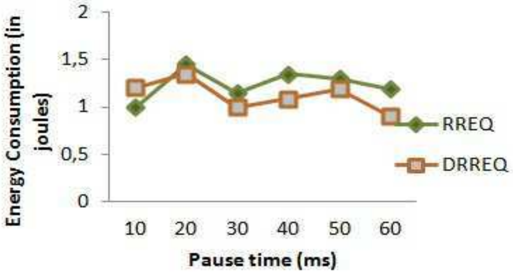


FIGURE 3.30 – *Energy consumption vs pause time*

energy and delay compared to the classic protocols.

The future work will consist to restrict the angle of directional antenna to multiple parts and to analyze the performance of nodes in the same metrics in mobile Ad hoc Networks.

As an application of presented functionalities, we propose an architecture in the next section for applying the routing and localization functions. This architecture is discussed to be used in the grand mosque of Elhajj. The application is based on the BSN for the health control and localization of pilgrims.

ABSTRACT

"The season of EL-Hajj is full of numerous problems that present a fertile field for application of new technologies like WSN. The following section describes an architecture for the use of WSN for medical application (BSN) in the Grand Mosque area for health control, localization and tracking of pilgrims."

3.5 Health Monitoring and Localization of Pilgrims in Real time : BSN Application in the Grand Mosque in Hajj

3.5.1 INTRODUCTION

Hajj (pilgrimage) is a huge gathering of Muslims on the earth. It is characterized by a place of their meeting and the kind of rituals they perform. This generates a series of challenges for the authorities to control the crowd and identify individuals. Therefore, the season of El Hajj becomes more difficult, especially when the whole crowd is the same movements at the same times do essentially the same thing. This spiritual gathering causes a lot of challenges and problems in relation to the conduct of rituals of El hajj. This is face to the increasing demand for good organization, security and control, the Hajj task remains one of the big challenges that Saudi authorities are facing each year. To this end, the authorities and officials are introduced to minimize these difficulties, especially those which may affect their health and life. Being different, some difficulties which may be mentioned are :

- Identification of pilgrims (lost, dead, or injured)
- Medical Emergencies
- Guiding lost pilgrims to their camps.
- Loss of identity documents and money
- Crowd control

As an emerging technology, WSN (Wireless Sensor Networks) composed from a large number of small, low data rate and inexpensive node that communicate in order to sense or control a physical phenomenon. WSN have a lot of applications like disaster management, health, military and security, and enormously attracted the community of researchers and has fueled the interest in sensor networks during the past few years. Sensors are typically capable of wireless communication and able to solve several problems in numerous domains. During the Hajj season, the organizers faced a lot of problems related to the health of pilgrims and their position in the area of El Hajj. At this time, the proposed works are focused on the identification of pilgrims lost, using the implementation of RFID (Radio Frequency IDentification). The latter solution, is as expensive equipment, requires adding tags to pilgrims. Those tags are limited to read data from those passives tags. Further work is limited only to the location of pilgrims. However, the aim of this paper is to discuss and propose a system which allows monitoring of pilgrims. Indeed, this allows, using a BSN (Body Sensor Network) as a particular application of wireless sensor network, for the localization of pilgrims lost and control, in real-time, the health status of those who fall into critical situation with diseases that could threaten their health and life. In this system, the agents in El Hajj, dispatched to several areas of Hajj and have devices that install applications to monitor and locate pilgrims, periodically, by reading sensors measurements in addition to their localization with adequate and theoretical technique. This solution, present a model for an area, and which can be duplicated for the full area of El hajj. It also facilitates the intervention and localization, in real time, of pilgrims who are away from their camps and to save their life.

3.5.2 RELATED WORKS

[72], the authors propose a prototype RFID-based Pilgrim Identification System, tested with a group of 1000 pilgrims from. This experiment proved to be very successful in demonstrating the effectiveness of RFID system in removing bottlenecks of the traditional authentication system. This work needs more investigation, especially for improvement of antennas design, selection of readersâ location, and communication frequency are also to be tackled. The same author [73], describes a developed system (Figure 3-31) for pilgrim tracking and identification using a mobile phone. The system consists of software that can be downloaded to the mobile phone of every pilgrim upon arrival to the Kingdome of Saudi Arabia. In add, the RFID tag can be programmed and be placed in inside the mobile. The mobile uses the Internet or SMS to send location information to a server managed by Hajj authority and to a server managed by the guide of the group that the pilgrim belongs to.

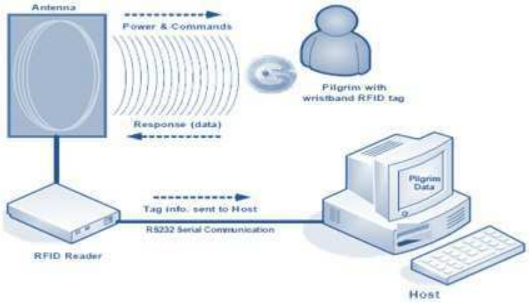


Figure 3.31 – *RFID System for pilgrim identification*

[74] Lists a project build by the use of WSN ; they made WSN Stations as emergency fixed stations. These stations are spread around the holy mosque to support local rescues and aid the retrieval of missing pilgrims. Each station has a button switch to press if the pilgrims get lost or if they need to request services. The last work is focused on the problems of missing people and helping those in need of urgent medical services with absence of any health control.

[75], propose an integrated solution to the problem of pilgrimage transportation control while tracking the shuttle-bus from its starting point till its final destination. The application identifies a particular bus by the RFID tag fixed on it. Passengers boarding or getting down the bus are identified on the basis of RFID cards

they have and finger identification.

[76], Yamin proposed a framework (Figure 3-32) which combines database and wireless technologies, by collecting pilgrim informationâs since her visa application, after the arrival and during the Hajj process ; for this, the author propose a mobile reader and scanner.

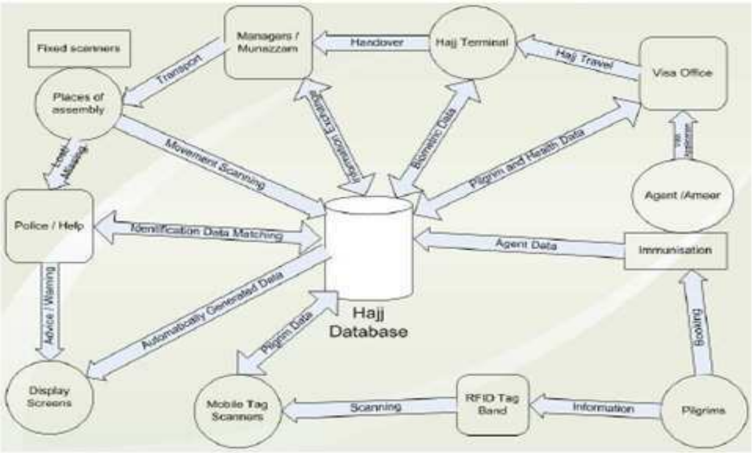


FIGURE 3.32 – *Framework for Hajj management*

3.5.3 WIRELESS SENSOR NETWORKS

WSN : Roles and Applications

Micro-electromechanical systems, embedded technology, sensor technology and wireless communication technology has become more sophisticated and progressive, to promote wireless sensor networks (WSN) generation and development, WSN become the current research in the field of IT hot, and has been widely used in many fields. Actually, this technology is omnipresent in application that requires communication with their components to transmit relevant quantities or values like light, temperature, humidity and more.

A WSN, sensor nodes are organized into fields "sensor fields" (Figure 3-33). Each of these nodes has the ability to collect data and transfer them to the gateway node (called "sink" in English or sink) via a multihop architecture. Well then transmits this data via the Internet or satellite to the central computer "Task Manager" to analyze and make these decisions.
Their applications are mainly related to conduct surveillance and remote control of the events of sensory (or physical) several different such as temperature, pressure, light, sound. These devices (motes or sensors) are able to capture and collect information sensitized in the environment monitoring , and then you send it wirelessly from one sensor to another in cooperation with each other to the base station (sink), which is a computer that collects information from wireless sensors scattered, processed and analyzed.

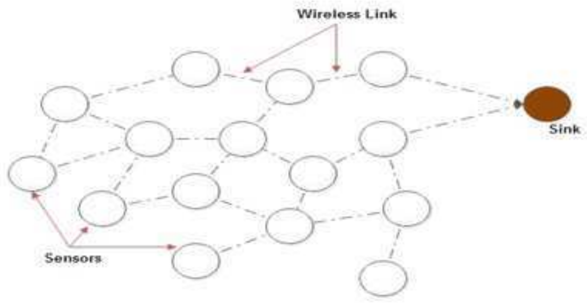


Figure 3.33 – *Sensor field architecture*

Due to their importance, sensors are used in many domains like military, rescue and ambulance, in nuclear reactors conducts a periodic surveillance, transport (plane and car) VANETs (Vehicle Ad hoc Networks), animal control, natural disasters (earthquakes and volcanoes) for the purpose of surveillance.

WSN : Challenges And Constraints

The main factors influencing the architecture and constraints of sensor networks can be summarized as follows :

• Fault Tolerance : Some nodes may generate errors or stop working because of a lack of energy, a physical or interference.
• Scale : The number of nodes deployed for a project may reach one million. Such a large number of nodes generates a lot of transfers inter nodal and requires that the well "sink" is equipped with lots of memory to store the information received.

• Production costs : Often, sensor networks are composed of a very large number of nodes. The price of a node is critical in order to compete with a network of traditional surveillance. Currently a node does not often costs much more than $ 1. For comparison, a Bluetooth node, already known to be a low-cost system, costs about $ 10.

• The environment : The sensors are often deployed en masse in places such as battlefields beyond enemy lines, inside large machines, the bottom of an ocean, fields biologically or chemically contaminated. Therefore, they must operate unattended in remote geographic areas.

• Network topology : The deployment of a large number of nodes requires maintenance of the topology. This maintenance consists of three phases : Deployment, Post-deployment, and Redeployment of additional nodes.

• Material constraints : The main constraint is the physical size of the sensor. Other constraints are that energy consumption must be reduced so that the network will survive as long as possible, it adapts to different environments (extreme heat, water, ..), it is very durable and autonomous since it is often deployed in hostile environments.

• The media transmission : In a sensor network, nodes are connected by a wireless architecture. To allow operations on these networks worldwide, the transmission medium must be normalized. We mostly use the infrared (which is license-free, robust to interference, and inexpensive), Bluetooth and ZigBee radio communications.

Body Sensor Networks (BSN)

BSN is a special Body Area network (BAN) whitch considered as a technology that emerges as the natural byproduct of existing sensor network technology and biomedical engineering. Professor Guang-Zhong Yang was the first person to formally define the "Body Sensor Network" (BSN) with publication of his bookBody Sensor Networksin 2006 [77].

BSN technology represents the lower bound of power and bandwidth from the BAN use case scenarios. Actually, This kind of structure, usually, use cellular network (3G) or WSN infrastructure to transmit data concerning patient to the base station and to the doctor (figure 3-34).

Wireless sensing and communication have the potential for large applications in medicine. Body Sensor Networks are a specific and medical application of wireless sensor networks intended to operate in a pervasive manner for on-body applications [78]. Using this technology, it is possible to obtain measurements of heart rate, oxygen saturation, pressure, and temperature, with small, non-invasive sensors ; we expect that, over time, an increasing array of sensors with sophisticated capabilities will become available.

Practically, BSNs for healthcare monitoring appears in several network applications operating in a variety of different environments including a hospital operating room, an elderly health clinic or a personal home setting and also in special area in hajj environment or in Kumbh Mela in India. Each of these environments varies substantially from one to another. Because of this, BSN framework must be adaptable and distributed to accommodate for such different settings. Due to this, we must appropriately structure the network in terms of number of sensors, and select relevant features in the BSN. Several benefits of the use of BSN can be exploited to monitor and control persons in real time and in their position.

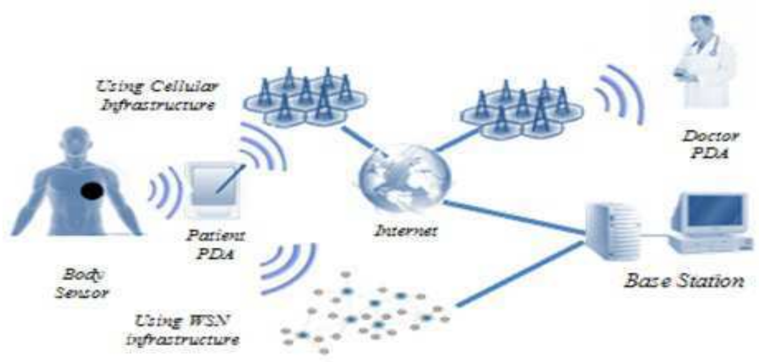


Figure 3.34 – *Sample of Existing BSN Architecture*

The Localization Challenge in WSN

Node localization is a complicated and important problem for wireless sensor networks (WSN). The aspects of this problem that have challenged the research community can be summarized as follows :

• Assumptions - The node localization problem remains a difficult challenge to be solved practically. To make the problem practically tractable, its complexity had to be reduced, by making simplifying assumptions. As a result, many localization schemes proposed solutions that are based on assumptions that do not always hold or are not practical. Examples of such assumptions are : Circular radio range, symmetric radio connectivity, Additional hardware (e.g., ultrasonic), lack of obstructions, lack of line-of-sight, no multipath and flat terrain.

•Localization Protocol Design - The problem of localization in WSN is further complicated by the large number of parameters that need to be considered when designing a localization system for a particular WSN deployment. Among these parameters are : the deployment method for the sensor network ; the existence of a line-of-sight between sensor nodes and a remote, central point ; the time required by the localization scheme ; the presence of reference points (anchors) in the network, and the density ; the cost for localization, represented by additional hardware (form factor) and energy expenditure (messages exchanged or time necessary for localization).

Sensor network localization algorithms estimate the locations of sensors with initially unknown location information by using knowledge of the absolute positions of a few sensors and inter-sensor measurements such as distance and bearing measurements. Sensors with known location information are called anchors and their locations can be obtained by using a global positioning system (GPS) [79], or by installing anchors at points with known coordinates. In applications requiring a global coordinate system, these anchors will determine the location of the sensor network in the global coordinate system. In applications where a local coordinate system suffices (e.g., smart homes), these anchors define the local coordinate system to which all other sensors are referred. Because of constraints on the cost and size of sensors, energy consumption, implementation environment (e.g., GPS is not accessible in some environments) and the deployment of sensors (e.g., sensor nodes may be randomly scattered in the region), most sensors do not know their locations. These sensors with unknown location information are called non-anchor nodes and their coordinates will be estimated by the sensor network localization algorithm.

Several measurement techniques in WSN localization can be listed depending on their localization technique like :
– AOA : Angle-of-arrival measurements,
– TDOA : Distance related measurements
– RSS : Received Signal Strength
– POA : Power of Arrival (PoA) detection systems :
– FOA : Frequency of Arrival (FoA) detection system

3.5.4 CONTRIBUTION AND PROPOSED ARCHITECTURE

Problem statement

El Hajj is a gathering place of millions of pilgrims from around the world. Around the grand mosque of El Hajj, hundreds of pilgrims are lost each year while away from their camps and their families during the rituals of El Hajj. Others who have health problems may arise in severe situations, especially in large crowds and congestion, causing death in some cases. Even before efforts in health services by local and international authorities, unfortunately, it is difficult to monitor and intervene in time to save lives. As reported in the related works, numerous existing applications using RFID are focused just on the identification of pilgrims and listing their information. Others focus only on the localization of pilgrims lost. At this moment, none of these applications treat health monitoring of pilgrims in real time.

It is in this context, we propose a hybrid architecture based sensor networks using BSN and able to locate lost pilgrims.

The proposed BSN Architecture

The BSN architecture of the pilgrim health control system is designed in a hierarchical tree. The main component here is the Pilgrim equipped by Body Sensors considered as mobile sensor. We note here, that just pilgrim declaring that they suffer from health problem (Cardiac, Imbalance in pressure, temperature, etc.) who must be equipped by these sensors. Murals and fixed sensors in several placement of the area of the Grand mosque are used to achieve data to the centres.

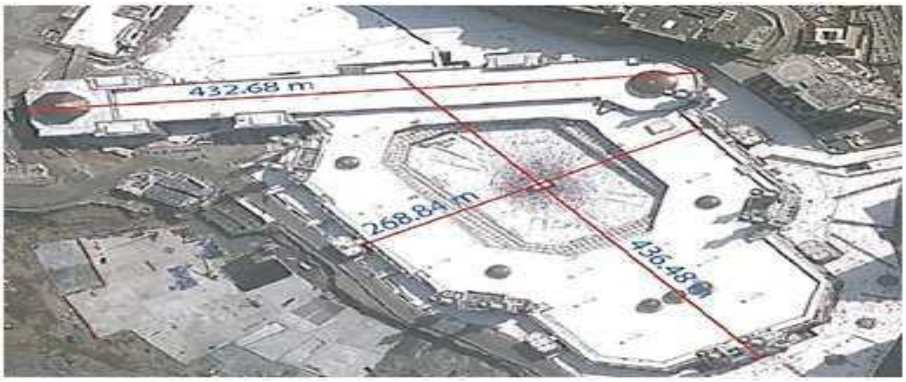


Figure 3.35 – *The Grand Mosque dimensions*

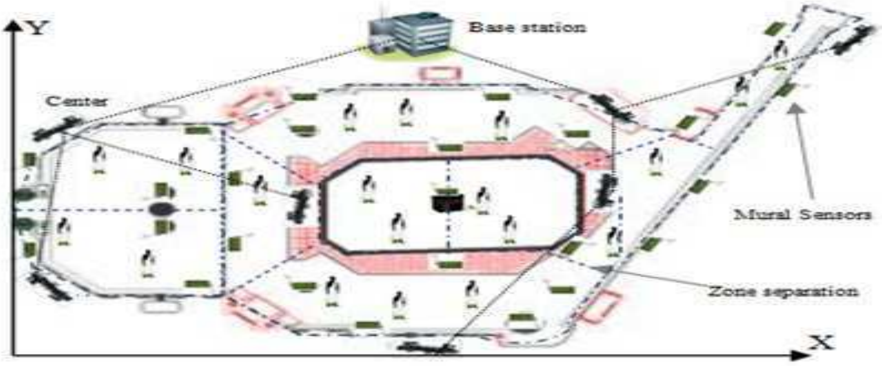


Figure 3.36 – *Sample of mural sensors deployment and zone repartition.*

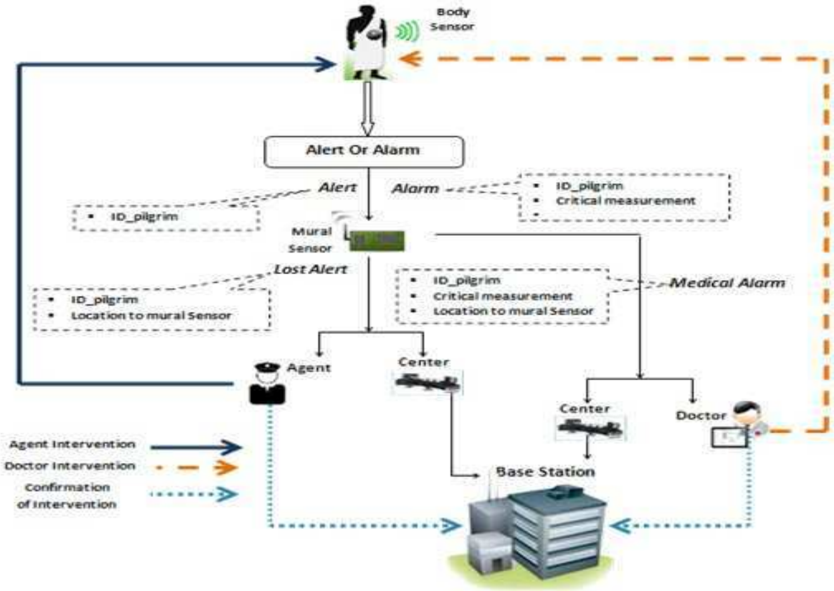


Figure 3.37 – *Illustration of pilgrim Alert/Alarm*

Those centres transmit valid request to base stations and to agents of their zone. The Grand Mosque area is subdivided to seven zones (Figure 3-36), each zone content a computer center that collect periodically measurement achieved by mural sensors. Taking in consideration the WSN rang and dimensions of the Grand mosque (Figure 3-35), those sensors are fixed and deployed to cover all area of the grand mosque, and referenced to absolute bi-dimensional reference (Figure 3-36).

The Body sensors send alarms when exceeding a threshold of critical measurements (Figure 3-37), by avoiding sending regular or periodic data, which causes more consumption of energy. This alarm is also sent to the doctor charged in the area. We note here that the agents and doctors in the area are equipped with information readerâs (Medical Alarm, Lost Alert) from the centers. Pilgrims lost can activate an alarm button, which sends an alert to the nearest wall sensor. The latter, inform both the center and agent of the area to which it belongs (Figure 3-37).

In another part, leaders of the camp may contact the base station or centres for any absence of pilgrims from his group, at that time ; an alert is broadcasted in the network to locate the pilgrim. Indeed, murals sensors play an important role by searching neighbouring sensor pilgrim sought : the sensor that find it, can locate it in relation to its reference, and then indicate its position to agent and centre of concerned area (Figure 3-38).
For pilgrim localization, the mechanism adopted is focused on broadcasting a ID_pilgrim request which refers to body sensor ID. The broadcasting is limited to the area (zone) of the mural sensor. The concerned ID sends a Replay to the near mural sensor. The latter, by routing mechanism, inform both agent and the center. We note her that the mural sensor that finds the ID, is considered as a reference by his position to locate the pilgrim lost.

Localization Technique

In the literature, several techniques are listed to locate a sensor, taking in consideration the optimization of the energy consumed to find this sensor ; we can list AOA, TDOA, POA [80]. Analytical method was listed in [81], this technique is adopted for large objet, and dedicated to transport domain and need a directional antenna for every sensor.

In this work, we use a fixed sensor in walls of El hajj areas, those sensors are considered as reference knowing their position. As mentioned in the Figure 3-38, we consider a mural sensor as reference who receive alert/alarm from the pilgrim sensor, the fixed sensor send this request to Agent/Doctor. The last receiver sends a request message to the pilgrim sensor in order to calculate the distances D1, D2 and D3 using (1) and (2) where C1 and C2 are defined in [5] and[81].

$$e^s_{ij} = C_1 + C_2 d^2_{ij} \qquad (1)$$

$$e^r_{ji} = C_1 \qquad (2)$$

We also use the AOA technique [80], by the triangularization method and using three other fixed mural sensors as references,

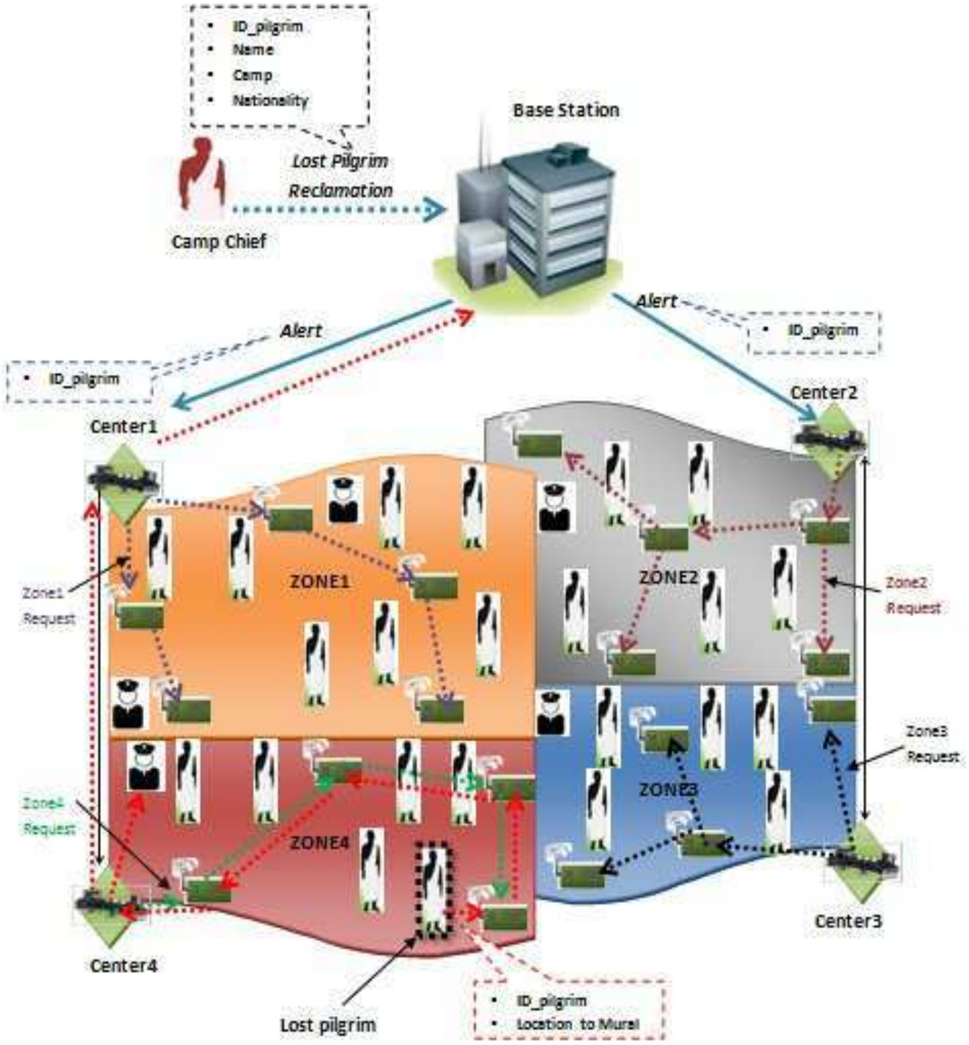


Figure 3.38 – *Illustration of Pilgrim Lost reclamation*

to know the angle between the fixed sensor and pilgrim. The measure, can easily used to deduce Xpi and Ypi where i=1, 2. We note that the direction (looked is from the agent/doctor to the pilgrim. Calculating D2, D3, can simply deduce that the pilgrim is same where on the circle C2 and same where on C3. The intersection between the two circles gives two probable positions (P1 or P2). To compute the direction to the pilgrim, we calculate it to the XAD position of Agent/Doctor : an analytical demonstration is given by the equations (3), (4) and (5).

$$X_0 =\mid Xpi - X_{AD} \mid \qquad (3.1)$$

$$\Delta_i = \sqrt{(\mid Xpi - X_{AD} \mid)^2 + Y_{pi}^2} \qquad (3.2)$$

Hence $cos(\theta_i) = \frac{Y_{pi}}{\Delta_i}$ and $\Delta_i = Arcos(\frac{Y_{pi}}{\Delta_i})$ (4)
Hence the direction to the pilgrim is :

$$\varphi_i = \pi - \theta_i \qquad (5)$$

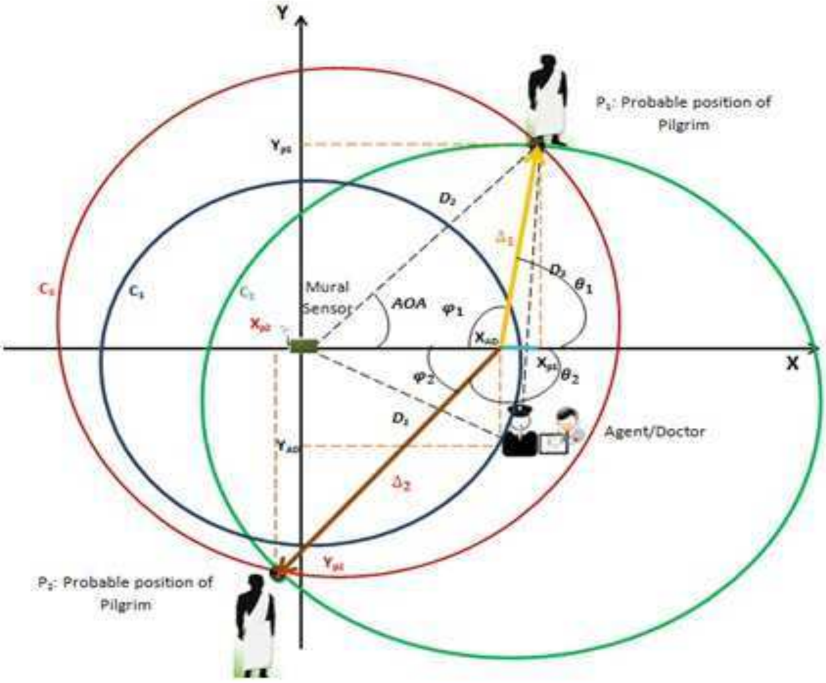
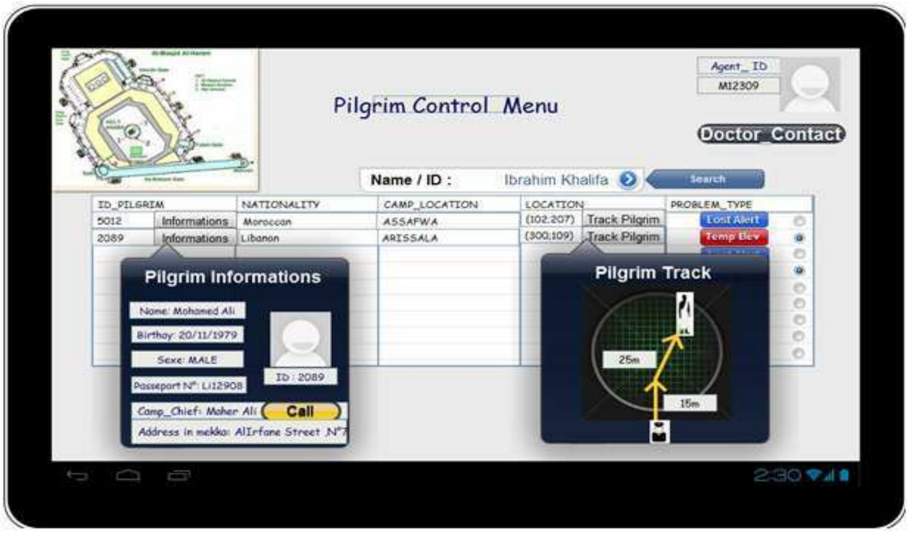


Figure 3.39 – *Localization technique illustration*

The values of serves to give the orientation and the direction to the lost pilgrim. The agent or the doctor, who uses a PDA, is oriented to the pilgrim, from the XAD as the initial point of the origin of direction to the destination. As mentioned in Figure 3-39, we have two possibilities of position of pilgrim, by the intersection of two circles. Using this technique, and to locate the real position in huge density of pilgrims in Hajj season, we consider the dichotomic approach discussed in [82], which use Dicho_AODV as a protocol with a specific RREQ (Route Request) mechanism based on discovery of destination on the right at first, the, on the left.

As described in the model (Figure 3-40), the agent/doctor equipped by an Ipad, which content informations about lost and patient pilgrim and also gives directions to them.



Pilgrim Control Menu

Agent_ ID: M12309

Name / ID : Ibrahim Khalifa

ID_PILGRIM		NATIONALITY	CAMP_LOCATION	LOCATION		PROBLEM_TYPE	
5012	Informations	Moroccan	ASSAFWA	(102:207)	Track Pilgrim	Lost Alert	○
2089	Informations	Libanon	ARISSALA	(300:109)	Track Pilgrim	Temp Elev	●

Pilgrim Informations

Name: Mohamed Ali

Birthay: 20/11/1979

Sexe: MALE

Passeport N°: Li12908

ID : 2089

Camp_Chief: Maher Ali

Address in mekka: AlIrfane Street N°7

FIGURE 3.40 – *Model of IPAD Pilgrim Control Application*

3.5.5 CONCLUSION

This work outlines a solution to one of the most problems in El hajj season related to the health, the control and localization of lost and special patients of pilgrims. The presented work were control the health of patients and locate the lost pilgrims in order to intervene in time to save lives and guide the lost pilgrims to their camps. This solution uses the BSN and the WSN technologies to control and achieve data to the base stations. An analytical localization technique is presented to locate both lost pilgrim and the patient in critical situation. An architecture and analytical study proposed here, in the perspective of an implementation and in-depth study in the environment of great mosque and with the authorities, for the development and deployment of this solution.

CONCLUSION PERSPECTIVES

4

ABSTRACT

"The next section gives a brief summary of the done work and the benefits of this thesis."

4.1 General Conclusion

In this thesis, we have presented the problem of energy optimization in sensor networks mainly in the relevant challenges as defined. Energy is one of researchersâ preoccupations in WSN. It is in this context that we kindly participated in the improvement of consumption in order to enlarge their spectrum use and lifetime. To achieve our goal, we acted on three axes ; security, localization and routing, which greatly affect the energy of sensors.

Indeed, in this work we presented a state of the art in WSN and their applications. In this section, we discussed the WSN, the WMSN and their architecture, the concept of QoS was addressed to the extent of its importance for signal validation and comparison of protocols, transmission standards and quality of communication. The security aspect was discussed because of its significance in the wireless communication and his effect on energy consumption and batteryâs sensors. Given its contribution to the energy optimization, routing was a colossal part of this report.

Subsequently, to obtain an optimal configuration, a series of colossal studies and contributions was presented for reporting and analyzes the foundations of the proposed functions. Firstly, we started with a comparative study to promote the technology UWB as an adopted function for WSN achieving large data in indoor space with better optimization of energy and delay. From another angle, a geometric and analytic technique for localization function was introduced in order to overcome the use of GPS which increases the size of sensor and depletes the battery. In the security functionality, a proposal hierarchical architecture based cooperative agent for the delivery of alerts following an intrusion. At the routing function, Dicho_AODV is a new protocol implemented in the NS2 simulator, proposed to avoid the wireless sensor overloading by the broadcast of route discovery message and therefore economize energy. This protocol is based on a dichotomic approach which acts on the mechanism of "hello message" broadcasting to discover destinations. This process was applied to the AODV protocol for the dissemination of RREQ messages with oriented and directional data. A last study was an interesting application conducted to design architecture for health monitoring and tracking pilgrims in the great mosque of El Hajj using the BSN and introducing hybrid realized work based on the dichotomic approach and localization of pilgrims.

The results, the completed and proposed studies show an energy economization and promote an improvement of the lifetime of these sensors in the context of their use. The done work and published results may be serving the research community to present more advances in this area. In this context, several authors use our papers as references and in their discussed works.

In fact, the domain of sensor network remains a fertile issue especially in the energy challenge. This axis knows an exponential development when other methods and energy resource will comes soon, for that scientific research and our participation will continue to serve humanity.

ABSTRACT

"Never the researches take End. It always opens new questions and new problems. In the next, the perspectives resulting from this thesis are enumerated for targeting the future works. It gives also a starting point for new searchers."

4.2 Perspectives Future Works

In spite of the advances in WSN domain, there are still many problems to be solved in this area affronting the constraints encountered. Despite the efforts made, the design of sensor networks still a very difficult task because it will combine the constraints specific to distributed systems and embedded systems.

Although the work that presented contributions to energy optimization in WSN, a number of issues remain to be studied. Thus, several research perspectives can be distinguished :

- Study of space and environment for implementing proposed solutions especially in places of Grand Mosque of El hajj and expand its use in el Harram.
- Develop an optimization mechanism of energy at the MAC level is a very important point and a further study.
- Investigations should be carried out both on how to formally specify the energy consumption in different levels of the protocol layer implemented in sensors.
- Move to act on the NS3 simulator which still open to be developed and being more competitive to other simulators for studying the energy consumption with more details.
- In the security, with our group, we are working for securing 6LowPAN architecture.
- Working on artificial intelligence, especially on neural networks for learning networks states and Bayesian networks to predict routes, and sensor behavior, to act on energy optimization, security and routing.

This non-exhaustive list of perspectives, that are available to us, shows that the area of research in this direction is very important. We hope to have shown that the optimization approach of energy in WSN is possible is paramount.

BIBLIOGRAPHY

[1] B. Yahya and J. Ben-Othman, "Energy efficient and QoS aware medium access control for wireless sensor networks" Concurrency Computat. : Pract. Exper. 2010 ; 22 :1252-1266 , April 2010,Wiley InterScience.

[2] Chih-Yung Chang *, Hsu-Ruey Chang, "Energy-aware node placement, topology control and MAC scheduling for wireless sensor networks", Computer Networks, Volume 52, Issue 11, 8 August 2008, Pages 2189-2204.

[3] Xianghui Fan, Shining Li, Zhigang Li, Jingyuan Li , "Sensors Dynamic Energy Management in WSN", Wireless Sensor Network, 2010.

[4] Cunqing Hua, Tak-Shing Peter Yum, "Data aggregated maximum lifetime routing for wireless sensor networks", Department of Information Engineering, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong, Journal Ad Hoc Networks, Elsevier, volume 6 Issue 3, May, 2008.

[5] Do Van Giang, Tarik Taleb,Kazuo Hashimito, Nei Kato and Yoshiaki Nemoto, A Fair and Lifetime-Maximum Routing Algorithm for Wireless Sensor Network, IEEE GLOBECOM 2007 proceeding.

[6] Ali Norouzi, Ahmet Sertbas, "An Integrated Survey in Efficient Energy Management for WSN using Architecture Approach", Int. J. Advanced Networking and Applications Volume : 03, Issue : 01-2011.

[7] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation base protocols for Disseminating Information inWireless Sensor Networks," Wireless Networks, vol. 8, pp.169-185, 2002.

[8] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy-efficientcommunication protocol for wireless microsensor networks", Proceedingsof the 33rd International Conference on System Sciences(HICSS '00), January 2000.
. [9] S. Lindsey and C. S. Raghavendra,"PEGASIS : Power-efficient gathering usingin sensor information systems," Proceedings of IEEE Aerospace Conference,vol. 3, pp. 1125-1130, Mar. 2002.

[10] Shigen Shen, Guangxue Yue, Qiying Cao, Fei Yu,A Survey of Game Theory in Wireless Sensor Networks Security, Journal of Networks, Vol 6, No 3 (2011), 521-532, Mar 2011,doi :10.4304/jnw.6.3.521-532.

[11] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security : a survey," IEEE Communications Surveys & Tutorials, vol. 11, 2009.

[12] R. Machado and S. Tekinay, "A survey of game-theoretic approaches in wireless sensor networks," Computer Networks, vol. 52, Nov. 2008.

[13] Amitangshu Pal, "Localization Algorithms in Wireless Sensor Networks : Current Approaches and Future Challenges", Network Protocols and Algorithms, ISSN 1943-3581, 2010, Vol. 2, No. 1.

[14] Guoqiang Mao, Baris Fidanb, c, c Brian D.O Anderson, "Wireless sensor network localization techniques", Elsivier, Computer Networks, Volume 51, Issue 10, 11 July 2007, Pages 2529-2553.

[15] Larios, J. Barbancho,F.J. Molina, C. León, "LIS : Localization based on an intelligent distributed fuzzy system applied to a WSN" Elsivier, Ad Hoc Networks Volume 10, Issue 3, May 2012, Pages 604-622.

[16] Xing-Hong KUANG, Hui-He SHAO, Rui FENG, "A New DistributedLocalization Schemefor Wireless Sensor Networks", Elsivier, Acta Automatica Sinica, Volume 34, Issue 3, March 2008, Pages 344-348.

[17] Yacine CHALLAL "Réseaux de Capteurs Sans Fil" -University of Technology in compiegne, France.

[18] CARTRON Mickael, "Vers une platforme efficace en énérgie pour les RCSF", Thesis presented in Rennes1 University, 2006.

[19] Potdar, V., "Wireless Sensor Networks : A Survey",International Conference onAdvanced Information Networking and Applications Workshops, 2009. WAINA '09,IEEEXPLORE ; 2009.

[20] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari "Energy-Efficient Communication Protocol for Wireless Microsensor Networks" Proc. of the 33rd Hawaii International Conference on System Sciences - 2000.

[21] KAZEM SOHRABY,Daniel Minoli,Taib Znati, " Wireless Sensor Networks Technology, Protocols, and Application" Wiley

Interscience BOOK, 2007.

[22] Ian F. Akyildiz,Tommaso Melodia,Kaushik R. Chowdhury "A survey on wireless multimedia sensor networks", Elsivier,Computer Networks, Volume 51, Issue 4, 14 March 2007, Pages 921-960.

[23] Changsu Suh , Zeeshan Hameed Mir , Young-Bae Ko,"Design and implementation of enhanced IEEE 802.15.4 for supportingmultimedia service in Wireless Sensor Networks ", Elsivier,Computer Networks 52 (2008) 2568-2581.

[24] Akyildiz, I.F.,"Wireless Multimedia Sensor Networks : Applications and Testbeds", IEEE Proceeding volume :96, Issue : 10, Oct.2008.
[25] Rita Cucchiara, Andrea Prati, Roberto Vezzani, "Using a Wireless Sensor Network toEnhance Video Surveillance"Journal of Ubiquitous, Computing and Intelligence,Vol.1, 1-11, 2006.

[26] E. Crawley, R. Nair, B. Rajagopalan, and H. Sandick. A Framework for QoS-based Routing in the Internet. Technical report, RFC 2386, 1998.

[27] Houarrii MAOUCHI "Routage avec Qualité de Service dans AODV",thesis presented in university Mouloud MAMMERI of tizi-ouzou.

[28] Mariam Dawoud, "Analyse du protocole AODV", DEA Memory Presented in Libanaise University, 2006.

[29] Azzedine Boukerche, "Algorithms and Protocols for Wireless Sensor Networks", Book inNovember 2008, Wiley-IEEE Press.

[30] Eren G{urses ö zgür B. Akan,"Multimedia Communication in Wireless Sensor Networks",Annales Des Télécommunication-sAugust 2005,Volume 60,Issue 7-8,pp 872-900.

[31] Imad Mahgouband Mohammad Ilyas, "Sensor Network Protocols" ,CRC Press2006,eBook ISBN : 978-1-4200-0634-6.

[32] Maria Gabriella Di Benedett, "Uwb Communication Systems : A Comprehensive Overview", Book Hindawi Publishing Corporation, 2006.

[33] HÃ$\frac{1}{4}$seyin Arslan, Zhi Ning Chen, Maria-Gabriella Di Benedetto ,"Ultra Wideband Wireless Communication",John Wiley & Sons.2006.

[34] Niels Hadaschik,"Techniques for UWB-OFDM" Available :

http ://www.iss.rwth-aachen.de/Projekte/theo.

[35] Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen "A Comparative Study of Wireless Protocols : Bluetooth, UWB, ZigBee, and Wi-Fi" Conf. of the IEEE Industrial Electronics Society (IECON) Nov. 5-8, 2007, Taipei, Taiwan.

[36] Karapistoli, Eirini ; Gragopoulos, Ioannis ; Tsetsinas, Ioannis ; Pavlidou, Fotini-Niovi "UWB Technology to Enhance the Performance of Wireless Multimedia Sensor Networks ", 2007. ISCC 2007. 12th IEEE Symposium on Computers and Communications.

[37] Chunsen Xu, Yanjuan Zhao, Yan Zhang in ,"Localization Technology in Wireless Sensor Networks Based on UWB" . International Conference on Wireless Networks and Information Systems (2009).

[38] T. Melodia, I F Akyildiz "Cross-Layer Quality of Service Support for UWB Wireless Multimedia Sensor Networks " in IEEE INFOCOM Conference on Computer Communications (2008).

[39] Berthe, A. ; Lecointre, A. ; Dragomirescu, D. ; Plana, R. "Simulation Platform for Wireless Sensor Networks Based on Impulse Radio Ultra Wide Band Networks" ICN '09. Eighth International Conference on Digital Object Identifier : 10.1109/ICN.2009.48 (2009).

[40] Jon Adams "Intelligent Systems Wireless Networking", Motorola Wireless and Broadband Systems. Available :
http ://archives.sensorsmag.com/articles/0603/14/.

[41] Jean-Yves Le Boudec,Ruben Merz,Bozidar Radunovic,Jörg Widmer "NS-2 (UWB) MAC and PHY simulator" Available :
http ://icawww1.epfl.ch/uwb/ns-2/index.html.

[42] Rachid Ennaji "Routing in Wireless Sensor Networks" 978-1-4244-3757-3/09/$25.00©2009IEEE-School of Science and Engineering- Al Akhawayn University in Ifrane, Morocco.

[43] F. Gustafsson, F. Gunnarsson, Mobile positioning using wireless networks : possibilities and fundamental limitations based on available wireless network measurements, IEEE Signal Processing Magazine 22 (4) (2005) 41-53.

[44] A.H. Sayed, A. Tarighat, N. Khajehnouri, Network-based wireless location : challenges faced in developing techniques for accurate wireless location information, IEEE Signal Processing Magazine , 2005.

[45] R. Kumaresan, D.W. Tufts, Estimating the angles of arrival

of multiple plane waves, IEEE Transactions on Aerospace and Electronic Systems AES-19 (1983) 134-139.

[46] R. Klukas, M. Fattouche, Line-of-sight angle of arrival estimation in the outdoor multipath environment, IEEE Transactions on Vehicular Technology 47 (1) (1998) 342- 351.

[47] B. Halder, M. Viberg, T. Kailath, An efficient non-iterative method for estimating the angles of arrival of known signals, in : The Twenty-Seventh Asilomar Conference on Signals, Systems and Computers, 1993.

[48] T. Rappaport, J. Reed, B. Woerner, Position location using wireless communications on highways of the future, IEEE Communications Magazine 34 (10) (1996) 33-41.

[49] Romit Roy Choudhury , Nitin H. Vaidya, "Performance of ad hoc routing using directional antennas", ELSEVIER, Ad Hoc Networks 3 (2005) 157-173.

[50] S.V. Schell, W.A. Gardner, High-resolution direction finding, Handbook of Statistics.

[51] G. Carter, Time delay estimation for passive sonar signal processing, IEEE Transactions on Acoustics, Speech, and Signal Processing 29 (3) (1981) 463-470.

[52] D. Koks, Numerical calculations for passive geolocation scenarios, Tech. Rep. DSTO-RR-0000, 2005.

[53] J.-Y. Lee, R. Scholtz, Ranging in a dense multipath environment using an UWB radio link, IEEE Journal on Selected Areas in Communications 20 (9) (2002) 1677- 1683.

[54] Al-Sakib Khan Pathan, Hyung-Woo Lee, "Security in Wireless Sensor Networks : Issues and Challenges", Feb. 20-22, 2006 ICACT2006, ISBN 89-5 519-129-4.

[55] Glenn Platt1, "The Tiny Agent- Wireless Sensor Networks Controlling Energy Resources", JOURNAL OF NETWORKS, VOL. 3, NO. 4, APRIL 2008
[56] J. Lopez and J. Zhou (Eds.) "Wireless Sensor Network Security", IOS Press, 2008.

[57] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, M. B. Srivastava, "on communication security in wireless ad-hoc sensor network", in : IEEE WETICE, 2002, pp. 139-144.

[58] H. Chan, A. Perrig, D. Song, "Random key predistribution schemes for sensor networks", in : IEEE Symp. Security and Pri-

vacy, 2003, p. 197.

[59] D. Liu, P. Ning, "Location-based pairwise key establishment for static sensor networks", in : ACM Workshop on Security of Ad Hoc and Sensor Netw., 2003, pp. 72-82.

[60] W. Du, J. Deng, Y. S. Han, P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks", in : ACM Conf. Computer and Commun. Security, 2003, pp. 42-51.

[61] Dimitrios Georgoulas, I"ntelligent Mobile Agent Middleware for Wireless Sensor Networks : A Real Time Application Case Study", 978-0-7695-3162-5/08, 2008 Crown.

[62] Peter Pecho, "Agent Platform for Wireless Sensor Network with Support for Cryptographic Protocols", Journal of Universal Computer Science, vol. 15, no. 5 (2009), 992-1006.

[63] Yoav Sasson David Cavin AndrÂ´e Schiper, "Probabilistic Broadcast for Flooding in Wireless Mobile Ad hoc Networks" Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE.

[64] Ch. Balaswamy, " An Energy Efficient Routing Protocol based on Periodic Route Discovery for Mobile Ad Hoc Networks", International Journal of Next-Generation Networks (IJNGN) Vol.3, No.1, March 2011.

[65] Carlos Henrique Pereira Augusto and JosÂ´e Ferreira de Rezende "Distributed Broadcast Scheduling in Mobile Ad Hoc Networks " Ad Hoc Networking Workshop (Med-Hoc-Net), 2010 The 9th IFIP Annual Mediterranean.

[66] LIU Wang-gui, QU Zhao-wei, "Scheme for on-demand route protocol in Ad-hoc networks" School of Computer Science and Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China, ELSIVIER September 2008, 15(Suppl.) : 41-45.

[67] Aminu Mohammed,Mohamed Ould-Khaoua,Lewis M. Mackenzie,Colin Perkins,Jamal-Deen Abdulai, "Probabilistic counter-based route discovery for mobile ad hoc networks", ACM Proceeding , IWCMC '09.

[68] K. Romer, The lighthouse location system for smart dust, in : Proceedings of MobiSys 2003 (ACM/USENIX Conference on Mobile Systems, Applications, and Services), pp. 15-30.

[69] Jamal-Deen Abdulai, Mohamed Ould-Khaoua, Lewis M. Mackenzie, "Adjusted probabilistic route discovery in mobile ad

hoc networks", Computers and Electrical Engineering 35 (2009) 168-182.

[70] Swapnil Shukla, "An Adaptive Probabilistic Routing Algorithm", thesis of INDIAN INSTITUTE OF TECHNOLOGY, KANPUR, May 2005.
[71] Chen Hongsong, Ji Zhenzhou, Hu Mingzeng, Fu Zhongchuan , Jiang Ruixiang," Design and performance evaluation of a multi-agent-based dynamic lifetime security scheme for AODV routing protocol", Journal of Network and Computer Applications 30 (2007) 145-166.

[72] Mohamed Mohandes, "Pilgrim Tracking And Identification Using The Mobile Phone, Ieee 15th International Symposium On Consumer Electronics 2011.

[73] Mohamed Mohandes, "An RFID-Based Pilgrim Identification System" 11th International Conference on Optimization of Electrical and Electronic Equipment (OPTIM), 2008.

[74] Mohamed Amer al nizar, " Emergency Stations in the grand mosque of Mecca using WSN", Master thesis , 2011.
[75] F. Abdessemed, Member IEEE, "An Integrated System for Tracking and Control Pilgrims Shuttle Buses", 14th International IEEE onference on Intelligent Transportation Systems, 2011.

[76] Mohammad Yamin, "A Framework For Improved Hajj Management And Research", International Conference on Wireless Communications and Sensor Networks, Dec 17-19, 2006.

[77] Guang-Zhong Yang, book titled : "Body Sensor Network" 2006.

[78] Yifeng He, "Optimal Resource Allocation for Pervasive Health Monitoring Systems with Body Sensor Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 11, NOVEMBER 2011.

[79] Guoqiang Mao, book chapter, "Introduction to Wireless Sensor Network Localization"2009.

[80] Guoqiang Mao "Wireless sensor network localization techniques", Elsivier, Computer Networks, Volume 51, Issue 10, 11 July 2007,

[81] Boudhir, Bouhorma Mohamed, Ben Ahmed Mohamed, "New Technique of Wireless Sensor Networks Localization based on Energy Consumption", JCA Journal 2010.

[82] Boudhir, Bouhorma Mohamed, Ben Ahmed, "New routing

protocol "Dicho-AODV" for energy optimization in MANETS", ICMCS 2012. Ieeexplore.

[83] Bani-Yassein M, Ould-Khaoua M, Mackenzei LM, Papanastasiou S. "Performance analysis of adjusted probabilistic broadcasting in mobile ad hoc networks", Int J Wireless Inform Networks 2006 ;13(April) :127-40.

[84] John Paul Walters, "Wireless Sensor Network Security : A Survey", 2006 Auerbach Publications", CRC Press.

A
Annexes

A.1 THE TOOL NS2

NS2 is an open-source event-driven simulator designed specifically for research in computer communication networks. It consists of OTcl and C++. The C++ objects are mapped to OTcl handles using TclCl. To run a simulation, a user needs to define a network scenario in a Tcl Simulation script, and feeds this script as an input to an executable file ns. During the simulation, the packet flow information can be collected through text-based tracing or NAM tracing. After the simulation, an AWK program or a perl program can be used to analyze a text-based trace file. The NAM program, on the other hand, utilizes a NAM trace file to replay the network simulation using animation. Simulation using NS2 consists of three main steps. First, the simulation design is probably the most important step. Secondly, configuring and running simulation implements the concept designed in the first step. This step also includes configuring the simulation scenario and running simulation. The final step in a simulation is to collect the simulation result and trace the simulation if necessary.

Written mainly in C++, NS2 employs a make utility to compile the source code, to link the created object files, and create an executable file ns. It follows the instruction specified in the default descriptor file Makefile. The make utility provides a simple way to incorporate a newly developed modules into NS2. After developing a C++ source code, we simply add an object file name into the dependency, and re-run make. NS2 is an object oriented simulator written in OTcl and C++ languages. While OTcl acts as the frontend, C++ acts as the backend running the actual simulation. As can be seen from, class hierarchies of both languages can be either standalone or linked together using an OTcl/C++ interface called TclCL. There are two types of classes in each domain. The first type includes classes which are linked between the C++ and OTcl domains.

In the literature, these OTcl and C++ class hierarchies are referred to as the interpreted hierarchy and the compiled hierarchy, respectively. The second type includes OTcl and C++ classes which are not linked together. These classes are neither a part of the interpreted hierarchy nor a part of compiled hierarchy. This chapter discusses how OTcl and C++ languages constitute NS2.

A.2 NS2 ARCHITECTURE

A.2.1 Node Architecture

A Node plays two important roles in NS2. As a router, it forwards packets to the connecting link based on a routing table. A Node is a composite object whose architecture is shown in Figure below.

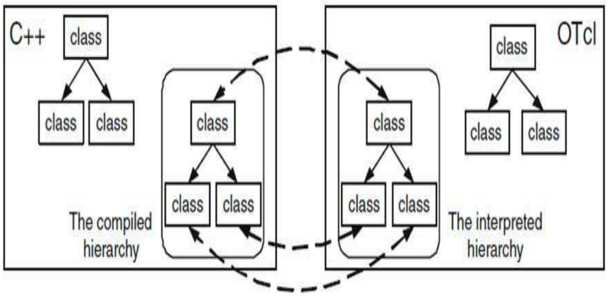


Figure A.1 – *Duality C++ OTcl In NS2 Architecture*

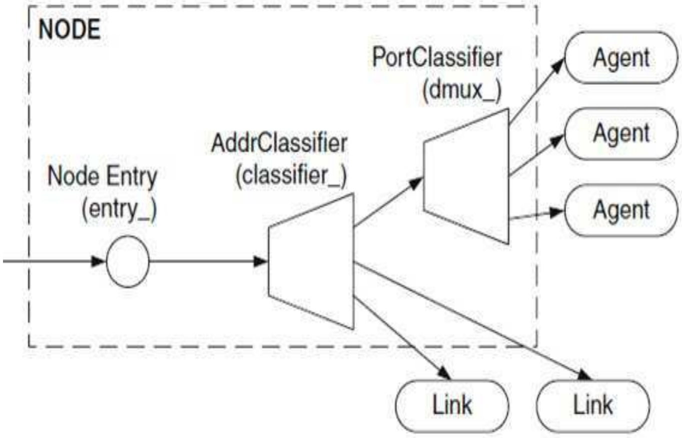


Figure A.2 – *Node Architecture in NS2*

A.2.2 NS2 Directory Structure

The package ns-allinone, in all versions, content several directories which are mentioned in the following figure :

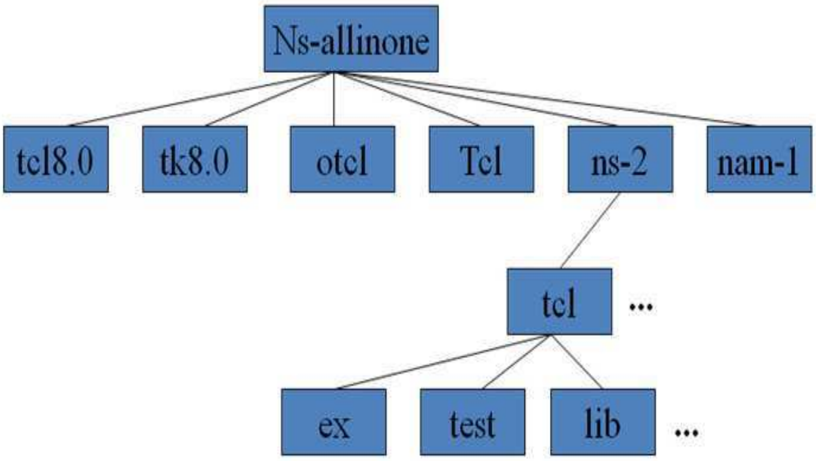


Figure A.3 – *Structure Of NS2 Directories*

A.3 INSTRUCTIONS FOR IMPLEMENTING THE DICHOAODV PROTOCOL

A.3.1 Description of a part of added directories and Files (.h, .cc)

A new directory âDichoAODVâ was created inside to NS2 base directory. Then we create five files there :

DichoAODV.h : header file where are defined timers and routing agent which performs protocolâs functionality.

DichoAODV.cc : file are actually implemented all timers, routing agent and Tcl hooks. DichoAODV pkt.h : this file content all packets DichoAODV protocol needs to exchange among nodes in the manet.

DichoAODV rtable.h Header file where our own routing table is declared. DichoAODV rtable.cc Routing table implementation.

To precise the type of packet, the Code below lists a part of this packet type used in DichoAODV :

```
DichoAODV/DichoAODV_pkt.h
#ifndef __DichoAODV_pkt_h__
#define __DichoAODV_pkt_h__
#include <packet.h>
#define HDR_DICHOAODV_PKT(p) hdr_DichoAODV_pkt::access(p)
struct hdr_DichoAODV_pkt {
nsaddr_t pkt_src_;
u_int16_t pkt_len_;
u_int8_t pkt_seq_num_;
inline nsaddr_t& pkt_src() { return pkt_src_; }
inline u_int16_t& pkt_len() { return pkt_len_; }
inline u_int8_t& pkt_seq_num() { return pkt_seq_num_; }
static int offset_;
inline static int& offset() { return offset_; }
inline static hdr_DichoAODV_pkt* access(const Packet* p) {
return (hdr_DichoAODV_pkt*)p->access(offset_);
}
};
#endif
```

To attach the packet header to Tcl interface, DichoAODV/DichoAODV.cc with the following code.

```
int DichoAODV_pkt::offset_;
static class DichoAODVHeaderClass : public PacketHeaderClass {
public:
DichoAODVHeaderClass() : PacketHeaderClass("PacketHeader/DichoAODV",
sizeof(hdr_DichoAODV_pkt)) {
bind_offset(&hdr_DichoAODV_pkt::offset_);
}
} class_rtProtoDichoAODV_hdr;
```

The next step is to implement the routing agent DichoAODV by the insert of functions,attributes used to achieve parquets.

```
DichoAODV/DichoAODV.h
#ifndef __DichoAODV_h__
#define __DichoAODV_h__
#include "DichoAODV_pkt.h"
#include <agent.h>
#include <packet.h>
#include <trace.h>
#include <timer-handler.h>
#include <random.h>
#include <classifier-port.h>
#define CURRENT_TIME
#define JITTER
class DichoAODV;
class DichoAODV_PktTimer : public TimerHandler {
public:
DichoAODV_PktTimer(DichoAODV* agent) : TimerHandler() {
agent_ = agent;
}
protected:
DichoAODV* agent_;
virtual void expire(Event* e);
};
class DichoAODV : public Agent {
friend class DichoAODV_PktTimer;
nsaddr_t ra_addr_;
DichoAODV_state state_;
DichoAODV_rtable rtable_;
int accesible_var_;
u_int8_t seq_num_;
protected:
PortClassifier* dmux_;
Trace* logtarget_;
DichoAODV_PktTimer pkt_timer_;
inline nsaddr_t& ra_addr() { return ra_addr_; }
inline DichoAODV_state& state() { return state_; }
inline int& accessible_var() { return accessible_var_; }
void forward_data(Packet*);
void recv_DichoAODV_pkt(Packet*);
void send_DichoAODV_pkt();
void reset_DichoAODV_pkt_timer();
public:
DichoAODV(nsaddr_t);
int command(int, const char*const*);
void recv(Packet*, Handler*);
};
#endif
```

Then, to assure the interfacing from TCL, because of this let DichoAODV to be instantiated from Tcl. For this, our agent has to be instantiated from the super class TclClass.

```
static class DichoAODVClass : public TclClass {
public:
DichoAODVClass() : TclClass("Agent/DichoAODV") {}
TclObject* create(int argc, const char*const* argv) {
assert(argc == 5);
return (new DichoAODV((nsaddr_t)Address::instance().str2addr(argv[4])));
}
} class_rtProtoDichoAODV;
```

For the use of the Timers, we have to program it to send packets and reset the timers after, see the code below added in DichoAODV/DichoAODV.cc :

```
void DichoAODV_PktTimer::expire(Event* e) {
agent_->send_DichoAODV_pkt();
agent_->reset_DichoAODV_pkt_timer()
}
```

In the file DichoAODV/DichoAODV.cc , DichoAODV PktTimer object is used to identify control packets sent and received by the protocol.

```
DichoAODV::DichoAODV(nsaddr_t id) : Agent(PT_DICHOAODV), \
pkt_timer_(this) {
bind_bool("accessible_var_", &accessible_var_);
ra_addr_ = id;
}
```

A.3.2 Description of main classes in the directional antenna

The code below describes the definitions of the directional antenna that use an angle between 0Â° and 180Â° to broadcast the RREQ : Directional Antennas

```
DirAntenna::DirAntenna()
{
char *antn;
char *token;
int i=0;
Gt_ = 1.0;
Gr_ = 1.0;
Angle_ = 0;
bind("Gt_", &Gt_);
bind("Gr_", &Gr_);
bind("Angle_",&Angle_);
bind("Width_",&Width_);
bind("Type_",&Type_);
/* calculate lower and upper angle */
lowerAngle = Angle_;
while(lowerAngle < 0){
lowerAngle += 180;
}
upperAngle = lowerAngle + Width_;
while(upperAngle < 0){
upperAngle += 180;
}
upperAngle %= 180;
lowerAngle %= 180;
solidAngleRatio = 2/(1 - cos(M_PI*Width_/180));
// Checking for the antenna type given
if (Type_ > 8 || Type_ < 0)
{
printf("Invalid antenna type given..should be between 0 & 8;\n");
exit(1);
}
if(Type_ != 0)
initialize_radiation_pattern();
}
void DirAntenna::setSAR()
{
//printf(" the current value of antenna parameters:\n");
//printf("------------------------------------------\n");
//printf("angle=%d, width=%d, solidangle=%f lower=%d
upper=%d\n",getangle(),getwidth(),getSAR(),getLA(),getUA());
lowerAngle = Angle_;
while(lowerAngle < 0){
lowerAngle += 180;
}
upperAngle = lowerAngle + Width_;
while(upperAngle < 0){
upperAngle += 180;
}
upperAngle %= 180;
lowerAngle %= 180;
solidAngleRatio = 2/(1 - cos(M_PI*Width_/180));
}
```

A.3.3 Mains changes In NS2 package

In the list of packet types in common/packet.h, we added PT$_{D}ichoAODVtothislistasmentionedbelow$:

```
enum packet_t {
PT_TCP,
PT_UDP,
PT_CBR,
/* ... ...... ... */,
PT_DICHOAODV,
PT_NTYPE
};
In the same file, wa added the name of packet type:
p_info() {
name_[PT_TCP]= "tcp";
name_[PT_UDP]= "udp";
name_[PT_CBR]= "cbr";
/* ... ...... ... */
name_[PT_DICHOAODV]= "dichoaodv"; }
```

To trace informations in a specific format, we add to the file trace/cmu-trace.h the lines :

```
class CMUTrace : public Trace {
/* ... ...... ... */
private:
/* ... */
void format_aodv(Packet *p, int offset);
void format_dichoaodv(Packet *p, int offset);
};
```

The Packet type must also be defined in the file tcl/lib/ns-packet.tcl as :

```
foreach prot {
DICHOAODV
AODV
ARP
# ...
NV
}{
add-packet-header $prot
}
```

The default value is defined in tcl/lib/ns-default.tcl :

```
...
Defaults defined for DichoAODV
Agent/ DichoAODV set accessible_var_ true
...
```

For the wireless simulation, we add the method create-DichoAODV-agent, and then we have to create in the file tcl/lib/ns-lib.tcl an instance of the protocol DichoAODV :

```
Simulator instproc create-wireless-node args {
# ...
switch -exact $routingAgent_ {
DICHOAODV{
set ragent [$self create-dichoaodv-agent $node]
}
# ...
}
Simulator instproc create-dichoaodv-agent { node } {
# Create Dichoaodv routing agent
set ragent [new Agent/ Dichoaodv [$node node-addr]]
$self at 0.0 "$ragent start"
$node set ragent_ $ragent
return $ragent
}
```

For the queue management, we add the lines below in queue/priqueue.cc :

```
Void PriQueue::recv(Packet *p, Handler *h)
{
struct hdr_cmn *ch = HDR_CMN(p);
if (Prefer_Routing_Protocols) {
switch(ch->ptype()) {
case PT_DSR:
case PT_MESSAGE:
case PT_TORA:
case PT_AODV:
case PT_DICHOAODV:
recvHighPriority(p, h);
break;
default:
Queue::recv(p, h);
}
}
else {
Queue::recv(p, h);
}
```

To compile the code and take into consideration all additions and modifications, we edit the Makefile like below :

```
OBJ_CC = \
tools/random.o tools/rng.o tools/ranvar.o common/misc.o \
common/timer-handler.o \
# ...
dichoaodv/dichoaodv.o dichoaodv/dichoaodv_rtable.o \
# ...
$(OBJ_STL)
```

A.4 Part of the NS2 code for Simulation using DichoAODV

The first part concerns the configuration of directional antenna :

```
# Parameters configured in directional antennas
Antenna/DirAntenna set X_ 0
Antenna/DirAntenna set Y_ 0
Antenna/DirAntenna set Z_ 1.5
Antenna/DirAntenna set Gt_ 1.0
Antenna/DirAntenna set Gr_ 1.0
```

```
Antenna/DirAntenna set Angle_ 0
Antenna/DirAntenna set Width_ 180
Antenna/DirAntenna set Type_ 0
```

options definitions

```
set val(chan)  Channel/WirelessChannel ;# channel type
set val(prop) Propagation/TwoRayGround ;# radio-propagation model
set val(netif) Phy/WirelessPhy ;# network interface type
set val(mac) Mac/802_15_4 ;# MAC type
set val(ifq) Queue/DropTail/PriQueue ;# interface queue type
set val(ll) LL link layer type
set val(ant) Antenna/DirAntenna ;# antenna model
set val(ifqlen) 50 ;# max packet in ifq
set val(nn) 6 ;# number of mobilenodes
set val(rp) DICHOAODV ;# routing protocol
set val(x) 100 # X dimension of topography
set val(y) 100 ;# Y dimension of topography
set val(stop) 150 ;# time of simulation end
set opt(engmodel) EnergyModel ;
set opt(txPower) 0.00175;
set opt(rxPower) 0.00075;
set opt(idlePower) 0.00005;
set opt(initeng) 10.0; # Initial energy in Joules

set ns [new Simulator]
set tracefd [open simple.tr w]
set windowVsTime2 [open win.tr w]
set namtrace [open simwrls.nam w]
$ns trace-all $tracefd
$ns namtrace-all-wireless $namtrace $val(x) $val(y)
# set up topography object
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)
#Create nn mobilenodes [$val(nn)] and attach them to the channel.
#
# configure the nodes
$ns node-config -adhocRouting $val(rp) \
-llType $val(ll) \
-macType $val(mac) \
-ifqType $val(ifq) \
-ifqLen $val(ifqlen) \
-antType $val(ant) \
-propType $val(prop) \
-phyType $val(netif) \
-channelType $val(chan) \
-topoInstance $topo \
-agentTrace ON \
-routerTrace ON \
-macTrace OFF \
-movementTrace ON\
for {set i 0} {$i < 5 } { incr i } {
set node_($i) [$ns node]
}
# Provide initial location of mobilenodes
$node_(0) set X_ 25.0
$node_(0) set Y_ 25.0
$node_(0) set Z_ 0.0
$node_(1) set X_ 30.0
$node_(1) set Y_ 35.0
$node_(1) set Z_ 0.0
$node_(2) set X_ 70.0
$node_(2) set Y_ 60.0
$node_(2) set Z_ 0.0
$node_(3) set X_ 90.0
$node_(3) set Y_ 40.0
$node_(3) set Z_ 0.0
$node_(4) set X_ 40.0
$node_(4) set Y_ 20.0
$node_(4) set Z_ 0.0
$node_(5) set X_ 10.0
$node_(5) set Y_ 5.0
$node_(5) set Z_ 0.0
# Generation of movements
$ns at 10.0 "$node_(0) setdest 70.075.0 30.0"
$ns at 15.0 "$node_(1) setdest 35.0 20.0 30.0"
$ns at 20.0 "$node_(2) setdest 60.0 15.0 30.0"
$ns at 30.0 "$node_(3) setdest 10.0 40.0 30.0"
$ns at 40.0 "$node_(4) setdest 30.0 90.0 30.0"
$ns at 60.0 "$node_(5) setdest 55.0 55.0 30.0"
# Set a TCP connection between node_(0) and node_(1)
set tcp [new Agent/TCP/Newreno]
$tcp set class_ 2
set sink [new Agent/TCPSink]
$ns attach-agent $node_(0) $tcp
$ns attach-agent $node_(1) $sink
$ns connect $tcp $sink
set ftp [new Application/FTP]
$ftp attach-agent $tcp
$ns at 10.0 "$ftp start"
# Printing the window size
proc plotWindow {tcpSource file} {
global ns
set time 0.01
set now [$ns now]
set cwnd [$tcpSource set cwnd_]
puts $file "$now $cwnd"
$ns at [expr $now+$time] "plotWindow $tcpSource $file" }
$ns at 10.1 "plotWindow $tcp $windowVsTime2"
```

```
# Define node initial position in nam
for {set i 0} {$i < $val(nn)} { incr i } {
# 30 defines the node size for nam
$ns initial_node_pos $node_($i) 30
}
# Telling nodes when the simulation ends
for {set i 0} {$i < $val(nn) } { incr i } {
$ns at $val(stop) "$node_($i) reset";
}
# ending nam and the simulation
$ns at $val(stop) "$ns nam-end-wireless $val(stop)"
$ns at $val(stop) "stop"
$ns at 150.01 "puts \"end simulation\" ; $ns halt"
proc stop {} {
global ns tracefd namtrace
$ns flush-trace
close $tracefd
close $namtrace
}
$ns run
```

Ce document a été préparé à l'aide de l'éditeur de texte GNU Kile et du logiciel
de composition typographique LaTeX 2_ε.

Ce document a été préparé à l'aide de l'éditeur de texte GNU Kile et du logiciel
de composition typographique $\LaTeX\,2_\varepsilon$.

Ce document a été préparé à l'aide de l'éditeur de texte GNU Kile et du logiciel
de composition typographique LATEX 2ε.

Your Comments here: