Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 1, 97-107 (2017)

www.astesj.com

Special Issue on Computer Systems, Information Technology, Electrical and Electronics Engineering

ASTES Journal

ISSN: 2415-6698

Cross layers security approach via an implementation of data privacy and by authentication mechanismfor mobile WSNs

Imen Bouabidi[1], Pr. Mahmoud Abdellaoui[*,2]

[1]WIMCS-ENET'COM, ENIS, Sfax University, Sfax - Tunisia,

[2]WIMCS-ENET'COM, Sfax University, Sfax - Tunisia,

ARTICLE INFO

Article history:
Received: 20 December, 2016
Accepted: 21 January, 2017
Online: 28 January, 2017

Keywords:
Mobile WSNs
Smart Sensors
MAC protocols
Data privacy
Malware and viruses detection
Authentication
Cross layers
Jamming attacks
OMNet++ simulator

ABSTRACT

To implement a new secure network with high mobility and low energy consumption, we use smart sensors. These sensors are powered by micro batteries generally non rechargeable. So, to extend their lifetime, it is necessary to implement new energy conservation techniques. Existing works separate the two features (security, energy conservation) and are interested specifically in only one layer.Consequently, the originality of this work consists to combine together the two features using a crossing between three layers: physical layer, data link layer and network layer. Our proposition consists firstly in developing a new network deployment in hierarchical areas. This model takes place at the network layer. Secondly, implementing an energy efficient and secure MAC protocol providing a secure authentication, data privacy and integrity in a mobile WSN. Finally, implementing an intrusion detection system protecting the physical layer from malware and viruses that threaten it. We have been used OMNet++ for simulation .Our proposed protocol SXMachiavel offered the best performances and more reliability at the mobility rate (can reach 99% compared with XMachiavel, which doesn't exceed 35%), loss packets rate (0.05% for a small network size) and energy consumption (decreases by 0.01% for each exchanged packet).

1. Introduction

To answer the specific questions proposed by academics-researchers and industrialists working in the wireless sensors network field and to have a mobile-secure and efficient WSN, our work is particularly concerned the security and the energy conservation of this network with mobile sensors [1-2].Indeed, we have implemented a cross layers security solution which provides data privacy and authentication for mobile WSN. We define WSN as a special type of ad hoc network, which usually consists of a number of nodes randomly deployed in an area to supervise or monitor diverse phenomena. The main difference between traditional networks and wireless sensors network is the scalability factor. In fact, WSN have thousands of nodes (more than 125000 nodes). This particular feature offers the possibility of an infinity path's number, which solve the network congestion problem and breaking links.

In the literature and up to now, the existing security solutions aren't adopted to the wireless sensors network constraints. For this purpose, security and energy conservationmechanisms must be added to protect the network against intrusions and virus that threaten it. In this context, we propose solutions specific to WSN. These solutions are applied to mobile WSN. As a result, we focus in this work on the major issue of security in wireless sensors network such as: authentication, privacy, data integrity, virus and intrusion detection while maintaining minimal energy consumption. Recall that our work has as objectives: firstly, the organization of network with low energy consumption and high mobility. Secondly, the introduction of security techniques to protect WSN. Finally, the use of smart sensors [3]. These smart sensors stand out over traditional sensors by digital processing thanks to the addition of processor which simplifies network management. All nodes share the same properties; they are autonomous and intelligent sensors with significant storage and computing capacity over traditional wireless sensors.

*Corresponding Author: Pr. Abdellaoui Mahmoud, WIMCS-ENET'COM, (+216) 50429427 & mahmoudabdellaoui4@gmail.com

Existing works in security and energy conservation are separated. They are interested only in the security theme or in the energy conservation theme without making the fusion between the two concepts. There are superficial solutions that aren't explored. Also, the majority of these works exploit the single-layer strategy and each solution deals with a particular layer and forgets the residual of the protocol stack. These works are limited on particular attacks which is insufficient to protect the entire WSN. To surmount these limitations, our solution is installed. It consists in merging both concepts security and energy conservation together in a crossing between three layers: physical layer, data link layer and network layer. This fusion doesn't exist in the existing works which separate the two issues. Indeed, the cross-layers design represents an interesting solution to address the security problem while guaranteeing a low rate of resource consumption.

To provide a complete security solution, our work is divided into three levels. A first level already made and published deals with network layer [4-6]. It consists of a network deployment in hierarchical areas. A second level is interested in the data link layer and especially in MAC sublayer through the development of an energy efficient and secure MAC protocol called SXMachiavel[7]. A last level concentrates on the physical layer by the implementation of an intrusion detection system at the sink level to protect the physical layer against Jamming attacks.

2. Energy conservation and security tools

Security and energy conservation are two essential elements in the wireless sensors network design. Therefore, our main objective consists in combining these two parameters to develop a generic and efficient sensors network. In the literature, these two themes are separated. Existing research works are focused either on the first theme or on the other theme. Consequently, the originality of our work consists in using these two parameters (energy conservation and security) at the same time in order to manufacture a complete security solution that meets the WSN requirements. Our solution is based on the crossing between the three layers:physical layer, data link layer and network layer.Up to now, these two fields are separated. Researchers are interested either in the security theme or in the energy conservation theme without making the fusion between the two. In fact, MAC protocols are divided into four types. Protocols basing on TDMA access: there are classic algorithms of slots reservation. These approaches seem to be complex, and present problems with the scalability factor like TRAMA protocol [8]. Then, protocols using CSMA access mode: these protocols, which use the contention period, are the most popular and represent the majority of MAC protocols proposed for wireless sensors network. But, they suffer from the latency when nodes are in sleeping mode; nodes have to wait until the receiver wakes up before they can forward a packet. SMAC, TMAC [9] and BMAC [10] are examples of this category. The third group is hybrid protocols: in spite of they try to combine points of TDMA and CSMA based protocols, these techniques seem to be complex such as ZMAC protocol [11]. The last type is inter-layers protocols. In order to minimize more the energy consumption, some researchers turn to the crossing between layers strategies and more exactly between MAC and network layers. One of the first inter-layers protocols is MAC CROSS [12]. These approaches are implemented with static sensors networks and they require the information of routing path from upper layer to determine the next hop. Afterward, nodes that aren't on the routing path go to sleep.

Turn now to present some existingsecurity mechanisms. The inherent characteristics of WSN, including wireless communication, random deployment and limited resources make it vulnerable against number of attacks. It is extremely easy for an intrusion to usurp the traffic circulating on the network. So, it comes necessary to protect the network. In the literature, some works were tried to solve security problems in the WSN. Generally, existing works were interested in saving energy, but they didn't address security of MAC protocols; some of them are concentrated in security against specific attacks such as a protection against Jamming attack at the physical layer level [13], or Wormhole attack in network layer [14]. On the other hand, some existing works take care well of network layer. Indeed, this layer is the module responsible for forwarding correctly a data from a point of network to another one. Thus, several authors go to the security of the routing path. Such as SecLEACH and SecPEGASIS protocols, which present the first solutions for securing hierarchical (cluster-based) networks with the dynamic clusters formation [15-16], also inwork [17] authors present a cross layers routing protocol. With the aim of providing an acceptable level of security, other researchers have developed either protocols assuring data confidentiality, such as DiDrip algorithm [18], techniques guaranteeing authentication and data integrity [19], or techniques providing secure data aggregation [20].Another research line turns to the cryptography aspects. The key management is one of these solutions. For such a system works and be secured each user must have a set of secret keys. In work [21], authors have implemented the encryption algorithm AES to protect data privacy in WSN. Other research theme is the intrusion detection system. For example, work [22] showed an implementation of IDS to secure the WSN. A final research line concerns the cross-layers strategies. The design cross layers represents an interesting solution to remedy the security problems while guaranteeing a low energy consumption. Work [23] explored the benefits of cross layers approach to overcome the single-layer protocols.

Our literature review of existing security and energy conservation techniques for WSN concludes with a comparison of the characteristics of each existing solution. This comparison shows that security is a complex problem. Each approach is characterized by its own needs and constraints that are required to achieve the desired security level. Indeed, existing security solutions are expensive in energy, memory space and don't offer the possibility of discovering new attacks. Moreover, the majority of works are based on the assumption that the WSN is static (all the used nodes are fixed). To remedy these limitations and to

reinforce the security level in the WSN some of them can be corrected and improved in order to manufacture a complete solution. It is *the cross layers approach*. At this stage, our solution settles down. It consists of a crossing between the three layers: network layer, data link layer and physical layer to provide a mobile and secure network. A detailed description of our contribution is explained in the next section.

3. Proposed Approach

As we have already said, our work deals with the security and energy conservation problems in the wireless sensors network. In the literature, *few works* are interested in the security aspect. According to our studies; we can notice that existent works in security and energy conservation terms present some drawbacks as following as: existing solutions are expensive in energy, in memory space and didn't offer the possibility of discovering new attacks. To overcome these limits our solution settles down. It consists of a crossing between three layers to provide a secure WSN. It has as objectives: firstly, the organization of a WSN with high mobility and low energy consumption. Secondly, the introduction of security techniques to protect the WSN. These security mechanisms should take in consideration the wireless sensors network constraints and limitations (limited memory capacity and computing). Finally, the use of intelligent sensors. Our contribution is based on three steps: the first step is interested in the network layer by developing a hierarchical network deployment that meets the requirements of this network. The second step is concentrated in the MAC sublayer through the development of an energy efficient and secure MAC protocol. The third step deals with the physical layer by implementing an intrusion detection system in order to protect physical layer against Jamming attacks.

3.1. Network deployment in hierarchical areas

Recall that the first step of our work deals with the network layer by constructing a new model specific and adapted to the WSN. In fact, the network layer is the module responsible for routing information to the right destination through a given connection network. Like ad hoc networks, wireless sensors networks are characterized by the absence of pre-existing fixed infrastructure. So, to ensure network connectivity, each node must participate in the routing, enabling it to discover existing paths and reach the other nodes of the network.

Our network model consists of a sensors network deployment in hierarchical areas. Indeed, the network structuring is one of the primordial tools to design the energy in each node which results in its lifetime prolongation. Hierarchical organization is a technique that consists in partitioning the network into subsets to facilitate its management and especially the routing which is realized at several levels. The literature has several contributions in the hierarchization techniques that can be classified into two types: areas and clusters. Clusters are defined as a set of nodes that have a node called a Cluster-Head (CH). This node acts as a relay between nodes in the same cluster and the base station or gateway. Generally, this node possesses higher energy resources compared to the other nodes. Clusters models suffer from some weaknesses. Indeed, the main disadvantage of the clustering approach is that it is mainly based on CH. So, if this node goes down all the approach becomes unuseless. To remedy this problem, the second approach appears. It is based on network partitioning into areas. In this context, we proposed a new network deployment in hierarchical areas. In our network model, areas are defined according to it carried radio which is equal to 400m and that can reach 8km by using plugging (SKY 65336, SKY 65337) and according to the number of jumps. This model presents some advantages: firstly, during the deployment phase all nodes have the same role and the same energy level. Then after, knots having important resources execute more complex tasks and knots having limited resources execute simple tasks. Also, this network model presents a large cover and high connexion and can improved reliability [4-6].

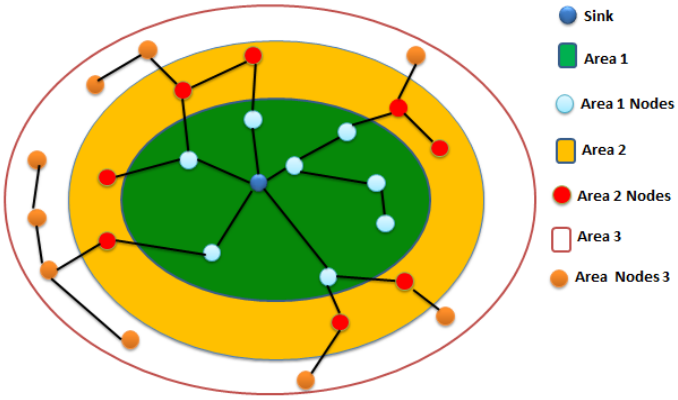

Figure1. Network topology

3.2. Secure Energy Efficient MAC protocol for mobile WSN

The data link layer and especially the MAC sublayer is mean subject of this step. The Media Access Control serves as an interface between software part that controls the link between nodes and physical layer. It controls the access management of multiple stations in a shared medium. In fact, each station listens to the medium before transmitting. If it is free, then the knot can send his data. If not, this knot either it passes in sleeping mode, or it waits its role. In absence of prevention mechanisms, this medium will be vulnerable against attacks and more exactly denial of sleep attacks. The adequate solution to fight against these attacks is the duty cycling technique. Among the existing energy conservation solutions, we choose the XMachiavel protocol. According to studies which were made, this protocol is the least energy consuming.We implemented this protocol in the existing MAC sublayer. Also, we developed an intrusion detection system in physical layer.These two methods increase network performances in security term. To validate our solution we used the OMNet++ simulator. Our work consists in implementing and adapting the XMachiavel protocol in our simulator. We supplied more details in the next section.

3.2.1. XMachiavel Protocol

Recall to modify and to ameliorate the XMachiavel protocol whose objective is to acquire a mobile and secure wireless sensors network. Consequently, we have chosen to use the existent MAC this protocol. According to the studies made and validated by simulations, this protocol is the most economical in energy. We implemented this protocol in the existing MAC sublayer using the OMNet++ simulator. OMNet++ doesn't support this protocol, so we have implemented and adapted the XMachiavel to our simulator. Figure 2 presents a description of its header.

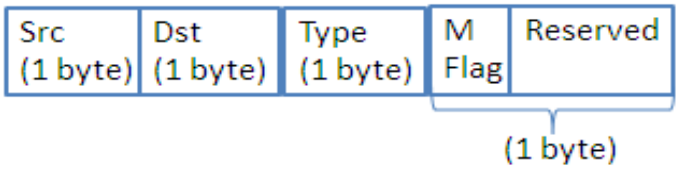

Figure 2. XMachiavel header [24]

- Src =Source node identifier,
- Dst = destination node identifier,
- Type: indicate whether a packet is a preamble, ACK or data,
- M Flag: used by the mobile node when it sends a data packet.

The header and preambles given in Figures 2, 4 and 5 improve the processing time; we present now a theoretical explanation of transmission and propagation time in a preamble MAC protocols

To include the effect of the preamble sampling technique, we present in this stage an adaptation and extension of classical CSMA analysis.A unicast DATA messagewill be preceded by a preamble of length T_P, and followed by an ACK message, as shown in Figure 3. If the ACK is not received, the message is repeated at a latertime [25].

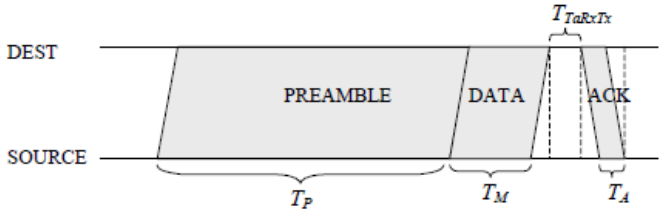

Figure 3. Data - ACK transaction using a wake-up preamble [25]

Transmission attempts at each node follow a random Poisson process with a mean rate g (mean inter arrival 1 / g). Therefore, the number of total transmission attempts will be the sum of the attempt of each node and correspond to a Poisson process of rate (N + 1) g, where N is the number of neighbors within a node. We will compute the throughput, the delay and the power consumption of the protocol in function of the mean rate g of the transmission attempts [25].

To calculate the power consumption of our protocol, wemust count the power consumption due to preamble sampling, the power consumption of listening to the medium when it is busy and the power consumption of transmitting [25].

Note that each node at a time t can take one of the following states: sleep state, channel listening state or transmission / reception state. The idle period starts at the end of the transmission of a packet and ends at the start of the next transmission. The duration of the idle period is a random variable $I = X + T_{TaRxTx}$, where X is the random time between the

end of the last transmission and the next arrival. Its cumulative distribution is [25]:

$$P(X <= x) = 1 - P(X > x) = 1 - e^{-(N+1)gx} \quad (1)$$

Giving a mean of

$$E[X] = 1/(N+1)g \quad (2)$$

Therefore, the mean duration of an idle period is

$$E[I] = 1/(N+1)g + T_{TaRxTx} \quad (3)$$

Turn now to the second state: the transmission/reception.This state is called a busy period. This period starts when the transmission starts and ends when the last interfering packet ends. Its duration is a random variable $_M B = Y + T$, where Y is the random time between the start of the first packet and the start of the last interfering packet.The mean busy period duration is presented by the following formulation [25]:

$$E[B] = T_M + T_P + T_{TaRxTx} - (1 - e^{-(NgTTaRxTx)})/Ng \quad (4)$$

Note that the proportion of the time when the medium is busy with non-persistent CSMA with preamble sampling is hence

$$b = E[B] / E[I] + E[B] \quad (5)$$

To simplify computations, we assume that a node will not stop listening as soon as the medium become idle, but will continue to listen until the next preamble sampling time. The proportion of listening periods will be equal to the proportion of busy medium given in formula (5).

Note that the processing time and the transmission time depend on the length of the frame. The longer the frame, the longer the processing and transmission times. According to Figure 3, we notice that the preamble length T_P is greater than the ACK length T_A .Consequently, the processing time of a preamble packet is more important than the processing time of an ACK packet.

However, XMachiavel protocol presents two weak points which are: first of all, it supports a low mobility. Then, it isn't secure: packets are sent unencrypted over the network. So, they can be easily intercepted by intruders. Also, it doesn't support any authentication, data privacy and integrity or intrusion detection mechanisms [26]. So, we are supposed to secure the packets exchange by introducing: firstly, an authentication mechanism. Secondly, a hash function guaranties the data integrity and finally, encryption process providing data privacy in the mobile WSN while increasing the mobility rate**.** A description of our improvement is detailed in the next section.

3.2.2 SXMachiavel protocol

Our solution consists in improving the existing MAC protocol XMachiavel by adding security mechanisms. A first part of our improvement is proposed at publication in [7]. It consists of:

- Increasing the mobility rate,

- Authentication mechanism by using a new field in each sent packet,
- Implementing of SHA1 as a hash function to provide the data integrity.

Firstly, we start by the authentication mechanism. It consists of adding a new field in each packet. We proceed by the following manner:

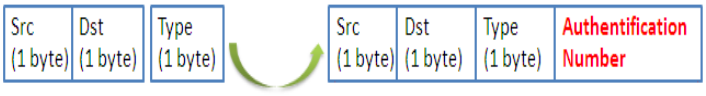

Figure 4. Preambles.

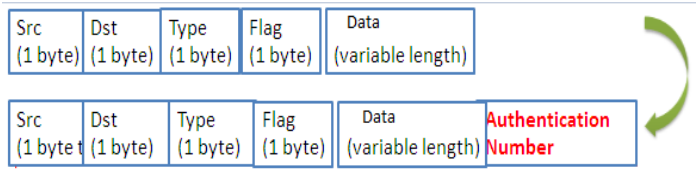

Figure5. Data Packet.

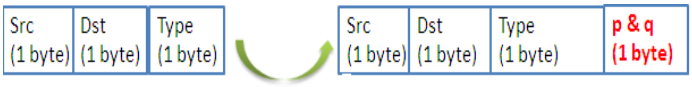

Figure 6. Acknowledgment

The authentication number is calculated as follows:

- A source node before sending a packet (preamble or data) generates two prime numbers p and q randomly [27].
- It calculates then the function f (n) = (p-1) * (q-1)
- The function f (n) corresponds to the AuthNum value (which will be added as a new field in each sent packet).
- The receiver calculates p and q from the received AuthNum value.

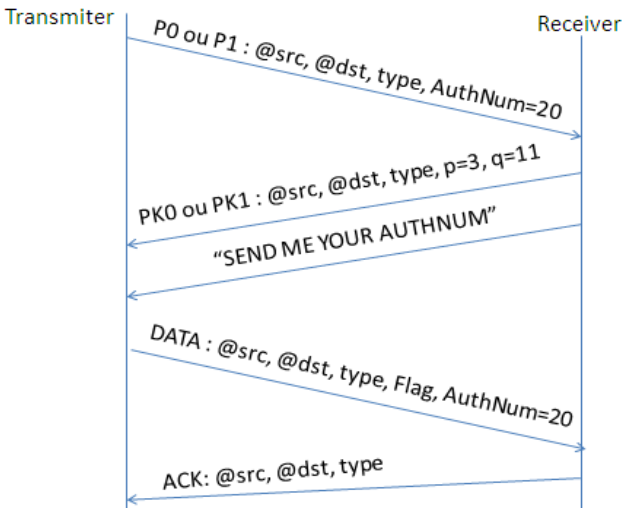

Figure 7. Sequence diagram of authentication process between two nodes

Two communicating nodes must authenticate firstly, so a sender node transmit an encrypted packet containing his identity which consist in the authentication number (AuthNum). Then, the receiver decrypts the packet and calculates the p and q values from the AuthNum value. Afterward, it sends an ACK packet and the message ‘’SEND ME YOUR AUTHNUM”. The transmitter then calculates AuthNum from the received values p and q. If the both values of AuthNum are equals, the source authenticates the destination and responds with a data packet containing the authentication number. Later, the destination node verifies the two value of AUTHNUM,if both values are equals, the sender will be authenticated. If not, the packet will be rejected.

Note that by adding authentication mechanism, the level of energy consumed in the network increases because the exchanges number between the transmitter and the receiver has increased. This increase is small compared to that obtained by the encryption mechanism. This will be approved by the simulation results presented in the next part.

With the aim of improving more the security level, the second step consists of: firstly, replacing the SHA1 hash function by a more recent and efficient hash function called SHA3 to provide the data integrity in the network [28]. Secondly, using the AES algorithm to guarantee the data privacy in mobile WSN [29]. Recall that the existent protocol XMachiavel doesn’t provide any security threats. Indeed,SHA3 is a new cryptographic hash function built on a principle completely different from SHA1 and SHA2 [28]. In previous work [7], we used SHA1. We present in the next section a comparison between SHA1 and SHA3 in term of loss packets rate and energy consumption. This function presents some security problems (collision attack). Weaknesses discovered on SHA1 raise fears of a fragility of SHA2 which is built on the same plan. SHA3 hash function uses the sponge constructionin which data is "absorbed" into the sponge and then the result is "squeezed" out. In the absorbing phase, message blocks are XORed into a subset of the state[28], which is then transformed as a whole. In the "squeeze" phase, output blocks are read from the same state subset, alternated with state transformations. The size ‘*r*’ of the state part that is written and read is called the "rate". The site ‘*c*’ of the part that is untouched by input/output is called the "capacity". The capacity determines the security of the scheme. The maximum security level is half the capacity. The hash function guarantees the data integrity. With this function, it is possible to determine the digest from the original message [28]. But, it is difficult to find another message that verifies the same function and gives the same digest. The receiver recalculates the digest and compares the two values. If they are different, the message is modified.

Turn now to the encryption method, we have used the AES algorithm. The AES (Advanced Encryption Standard) is a symmetric encryption standard to replace the Data Encryption Standard (DES), which has present limits in the face of current attacks. It operates on 128-bit blocks which it transforms into 128-bit encrypted blocks by a sequence of Nr operations or "rounds", from a 128, 192 or 256-bit key. Depending on its size, the number of rounds differs: 10, 12 and 14 rounds, respectively [29].The encryption process is described as following as:

- *BYTE_SUB (Byte Substitution)*: It is a non-linear function operating independently on each block from a so-called substitution table.
- *SHIFT_ROW:* It is a function that performs offsets (typically it takes 4-byte 4-bit input and shifts 0, 1, 2 and 3 bytes for bits 1, 2, 3 and 4 respectively) [30].
- *MIX_COL*: It is a function which transforms each input byte into a linear combination of input bytes and can be expressed mathematically by a matrix product on the Galois field (28).

The decryption process consists of applying inverse operations in reverse order and with sub keys also in reverse order.

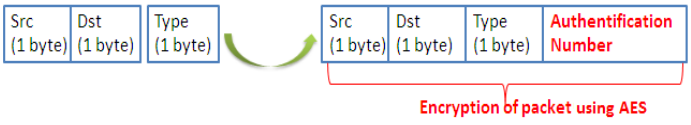

Figure 8.Encryption of Preambles using AES.

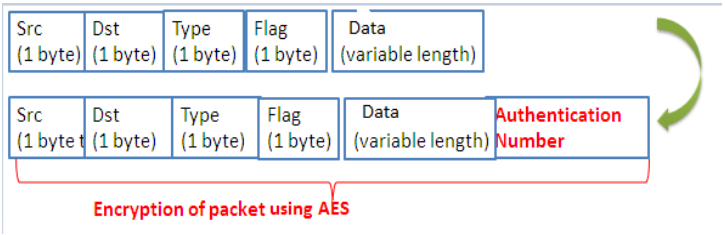

Figure 9. Encryption of data packets using AES.

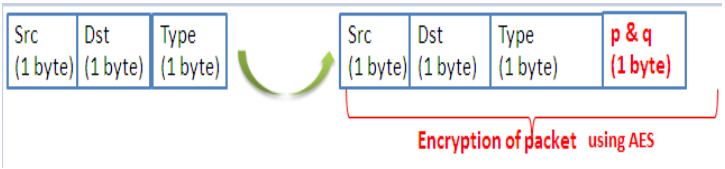

Figure 10. Encryption of acknowledgements using AES.

To secure the existing MAC protocol XMachiavel, we proceeded by the following way:

- ✓ Authentication mechanism that guaranties the authenticity of the network.
- ✓ A recent hash function called SHA3 that ensures the exchanged data integrity [31]. In our previous work, we have applied the hash function on all packets exchanged, whether preambles, ACKs or data [7]. But, according to simulations that were made, we observed the increase in the energy consumption rate. In addition, preambles and ACKs contain less important information's than data so; there is no need to apply the hash on these packets. As result, we gain at the energy consumption level.
- ✓ A symmetric encryption algorithm AES that guarantees data privacy in WSN. We apply this algorithm on all packets exchanged (preambles, ACKs and data) in order to limit the appearance of malware and viruses.

In transmission, the source node follows the following steps:

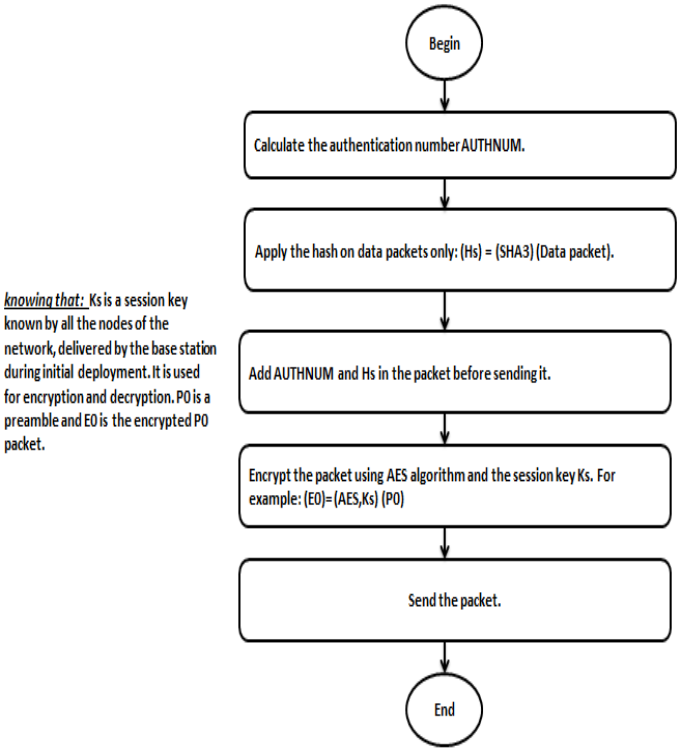

Figure 11. Security process followed by each node during the transmission

In reception, the destination node follows the following steps:

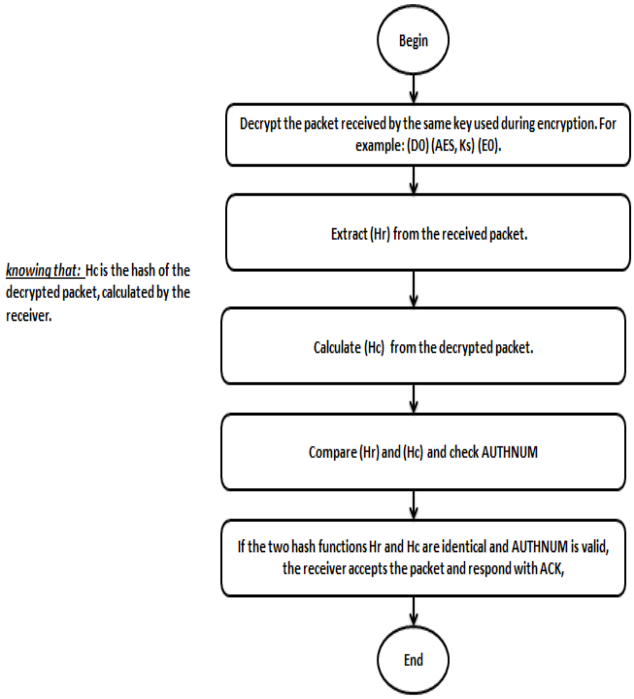

Figure 12.Security process followed by each node during the reception.

3.3. Implementation of an IDS to protect physical layer against Jamming attacks

As we have already said, our contribution consists in using a cross between the three layers: physical layer, data link layer and network layer to provide secure WSN. We have previously

specified our security solutions with regard to both data link and network layers. These approaches begin with the development of a new network deployment model in hierarchical areas. This model takes place at the network layer level and its goal is to provide an efficient and mobile WSN network. Next, we are focused on the data link layer and more specifically the MAC sublayer through the implementation of an energy-efficient MAC protocol that ensures secure authentication and data privacy in the WSN. Finally, in order to provide a complete and specific security solution to WSN, we address to protect the physical layer. The wireless sensors network is considered one of the communication technologies that have emerged over the years. Among the WSN features, we quote the wireless communication. As a result, the physical channel of this network is distinct from other traditional networks. For example, the fluctuations caused by an unstable wireless channel are more severe. These characteristics are considered as gaps that must be eliminated in the network design. Consequently, the security of the physical layer represents an interesting attitude. Indeed, the physical layer is the lowest layer in the OSI model. Its main role is to transmit and to receive the stream of unstructured raw bits on a physical medium.

In the last step of our work, we focus on how to ensure the security of the physical layer in the wireless sensors network. Existing security solutions are often implemented in the upper layers. In addition, the coexistence of the secure physical layer must be taken into consideration. Recall that this layer is vulnerable to attacks and specifically Jamming attacks. These malware and viruses attack wireless communication. Indeed, an attacker tries to interfere with the radio frequency used by the sensor nodes in the network. So and to eliminate these anomalies, we proposed as solution the implementation of an intrusion detection system. Despitethe IDSs are expensive in energy and the WSN is characterized by low memory capacity and limited energy, we chose to apply this IDS only at the sink node level. This node is responsible for detecting the anomaly and then informing the other nodes of the intrusion existence using a broadcast message or an alert and finally taking the prevention decision.

In the security field, we called intrusion any attempt to violate the security policy of a system. Precisely, it is the violation of the security services namely: data privacy, integrity or authentication. The network should continue to operate despite the appearance of unknown behavior likely to impede the proper network functioning. As example of intrusion we present Jamming attacks that threat the physical layer. In fact, the Jamming is a well-known attack that target wireless communication. Indeed, an adversary attempts to interfere with the radio frequency (interference) used by the sensor nodes in the network.

In Jamming, the nodes do not have access to the medium and cannot communicate because of the radio interference. However, a network without access to the medium is a network out of order so, the Jamming is a denial-of-service attack. This radio interference will have a direct influence on the values of several network parameters. Subsequently, increasing or decreasing the values of these parameters will be an indication of the existence of a Jamming attack. Then, these parameters can be used in the detection of these anomalies. These parameters include: PDR, PSR, ECA, LPR and CST [13].

-*Packet Delivery Ratio (PDR*): The PDR is defined as the ratio between the number of packets successfully delivered to a destination node and the number of sent packets by the sender node.

-*Packet Send Ratio (PSR):* The PSR is defined as the ratio between the number of packets sent successfully by a node and the number of packets it intends to send (messages in queue).

-*Loss Packet Rate (LPR*): The LPR is defined as the ratio between the number of packets lost and the total number of packets over a given period.

-*Energy Consumption Amount (ECA):* The ECA parameter is defined as the amount of energy consumed by a node for a specified period of time.

-*Carrier Sensing Time (CST):* In Medium Access Control (MAC) protocols, such as the Carrier Sense Multiple Access (CSMA) protocol, each node tries to detect when the media is free. So that it can then send its own packets. The period during which the node must wait for the carrier to become free is called Carrier Sensing Time (CST). This period is calculated as the average time elapsed between the moment when a node is ready to send its packet and the moment when the medium is released so that the node can send its packet.

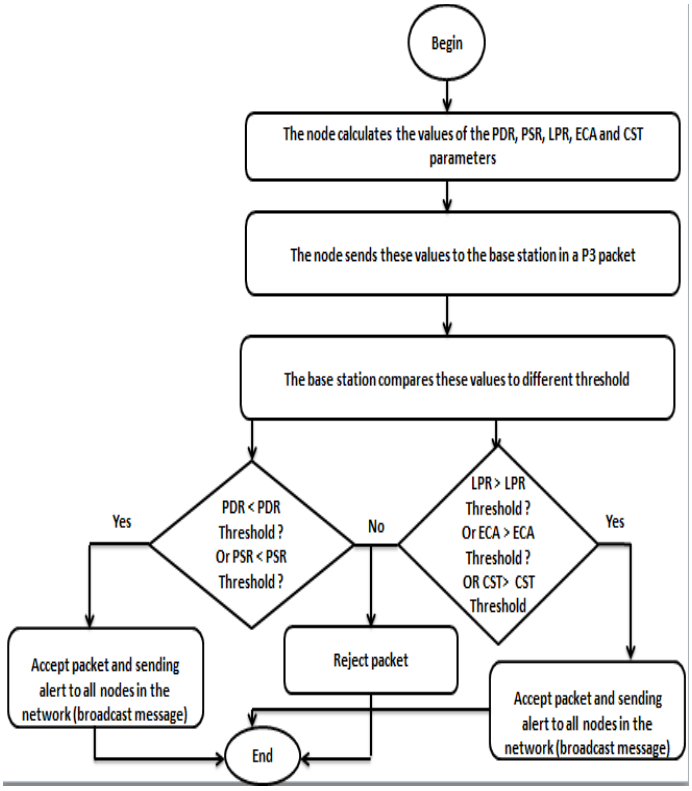

Figure 13. IDS process.

Existing works for detecting Jamming attacks use the combination of two, three, or up to four parameters. Such as the work [32] which use the four parameters PDR, BPR, RSSI and CCA to calculate the interference index. This calculation is done by each node. The CCA is a variable that counts the number of times the transmitter finds the channel busy trying to send a packet. The major disadvantage of this method is the necessity of complicated computation at the nodes, which is costly in energy terms. Other researchers use the parameters BPR, PDPT and SNR to calculate the Jamming index [21]. This method is able to solve the complex computational problem at the nodes, because all the computation is done by the base station. In our solution, we kept this solution by increasing the number of parameters to five. These parameters are: PDR, PSR, LPR, ECA and CST. Each node performs the calculation of each parameter for a given period and then sends these values to the base station which compares these values to the different thresholds. We proceeded as follows:

In our solution, we add a new packet P3 which containing the values of these parameters. Each node must encrypt the packet using AES and the session key Ks before sending it to the base station. The P3 fields are showed in Figure 14.

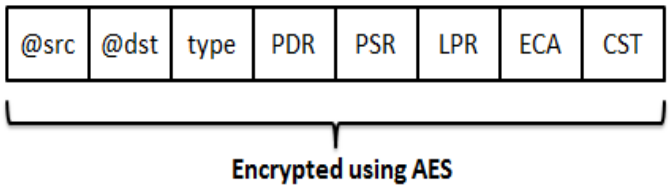

Figure 14. P3 fields

4. Simulation Results & Discussion

To evaluate the performances of both protocols XMachiavel and SXMachiavel, we use the simulation through OMNet++. For the case of our proposition, we used firstly SHA1 hash function; secondly, we change it to SHA3. We evaluate three metrics which are: mobility rate, loss packets rate and energy consumption.Before beginning the simulation, some parameters must be adjusted. First, we used a wireless sensors network with a topology of 500m * 500m with a random deployment of nodes. These nodes may be fixed or mobile nodes. For the XMachiavel protocol case, the percentage of fixed nodes is larger than the percentage of mobile nodes (see Table 1). On the other hand, the mobile nodes are more numerous than fixed nodes for the SXMachiavel protocol case. After each simulation duration(equal to150s), we incremented the number of nodes and we calculated the different metrics.

Table 1 detailed our simulation parameters.

4.1. Mobility rate

Before calculating the mobility rate, we present a histogram which indicates the partition of fixed and mobile nodes in the network for both protocols XMachiavel and SXMachiavel (using SHA1 or SHA3).

Table 1. Simulation parameters

Network size	*500m*500m*
Nic Type	*NicXMachiavel ; Nic SHA1SXMachiavel; Nic SHA3SXMachiavel*
Mobility Type	*ConstSpeedMobility*
Thermal noise	*-121dbm*
Carrier Frequency	*868e+6HZ*
Header length	*24 bits*
Queue length	*5*
Simulation Time	*150s*
Bit rate	*15360 bps*
Number of mobile nodes	*Variable (from 0 to 199)*
Number of fixed nodes for XMachiavel case	*Variable (from 0 to 149)*

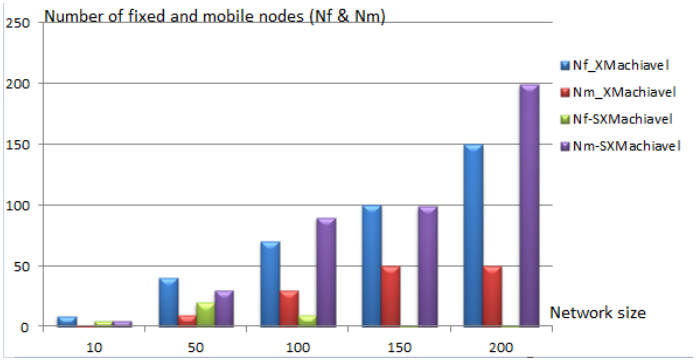

Figure 15. Number of fixed and mobile nodes in the network

Recall to: the mobility rate is the report between the number of mobile nodes and the total number of nodes in the network.

Mobility rate = Number of mobile nodes / Total number of nodes.

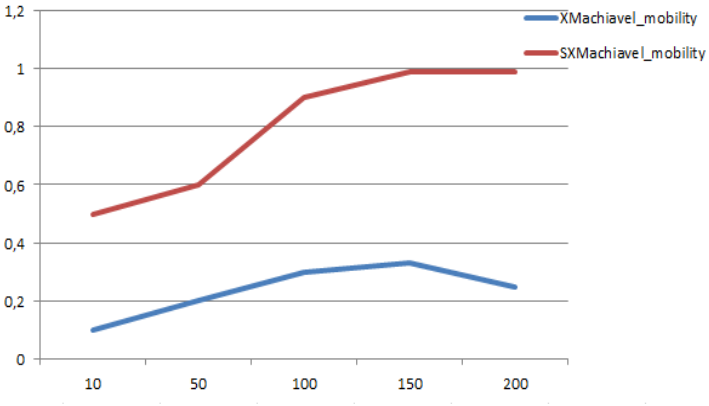

Figure 16.Variation of mobility rate according to network size

According to the Figure 16, we notice that mobility rate is different for both protocols. Recall that our objective is the developing of an efficient and secure WSN to combine the two metrics (energy conservation and security). So, we have increased the mobility rate in our approach. In the XMachiavel protocol, the number of fixed nodes is more than the number of mobile nodes (which doesn't exceed 50 nodes). But, it doesn't the case for our proposition which has as goal providing a totally mobile network. For this reason, we have increased after each simulation duration (= 150s) the total number of mobile nodes. From a network size 200, all the nodes will be mobile except the sink which remains

fixed. So, the mobility rate reached 99%. Subsequently, we achieved our goal which is providing a totally mobile network.

4.2. Loss packets rate

Recall to: the loss packets rate is the report between the number of lost frames and the total number of sent frames. To realize a correct simulation, we specified, at first, the simulation conditions (see table 1). Furthermore, we increased, every time, the number of knots to show the resistance of protocols with scaling factor. The formula is presented as following as:

Loss packets rate = Counts loss frames / Number of transmitted frames**.**

To evaluate the loss of packets, we performed several simulations between the non-secure protocol XMachiavel and our secure protocol SXMachiavel. The first simulation is done between XMachiavel and SXMachiavel with only the authentication mechanism. The results of this simulation are shown in the Figure17.

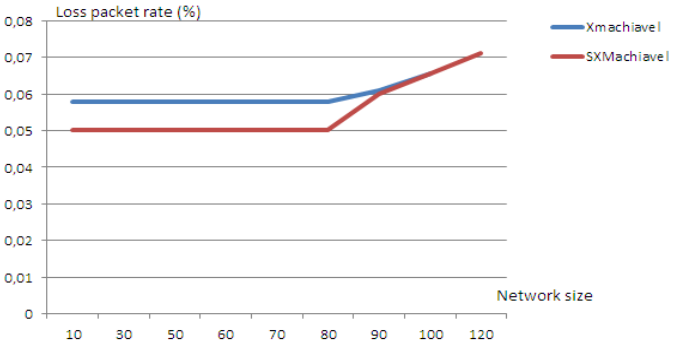

Figure 17**.**Variation of loss packets rate according to network size

The loss packets rate is 0.05% for a small network size (from 10 to 80 knots): a non-significant loss. Our network is completely secured (implementation of three security mechanisms as follow as: authentication - hash and encryption. Then, the risk of intrusion appearance is low. This explains the lack of packet loss (0% loss) for a small network (see Figure 18).

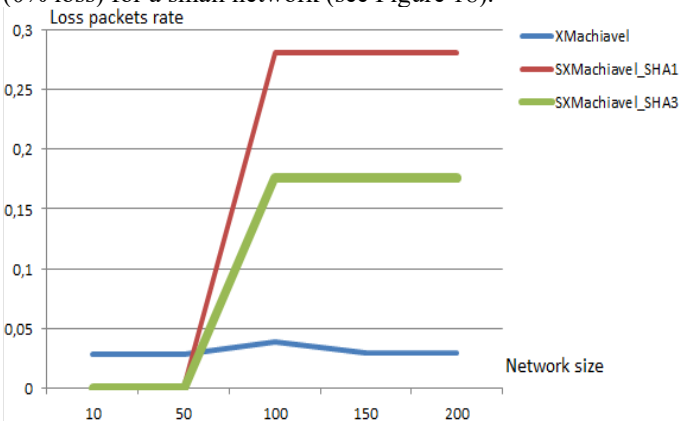

Figure 18**.**Variation of loss packets rate according to network size

As become famous in Figure 18, the loss packets rate increases with the number of nodes in the network. For a small network size (10 to 50), our proposed approach provides the best results (0%loss), but when the network size becomes vast, XMachiavel protocol shows the lowest loss packets rate. We explain these results by adding security mechanismsin SXMachiavel and the increase of number of packets exchanged. Indeed, the addition of security technologies increases the data transfer betweennodes and subsequently the loss of packets also increases. Turn now to compare between SXMachiavel protocol using SHA1 and SHA3, we note that the loss packets rate is higher in case of SHA1. Which demonstrate the fragility of this hash function to security attacks and shows the effeciency of SHA3 in terms of loss packets rate.

4.3. Energy Consumption

Recall to: Energy consumption = Transmission energy + processing energy + energy consumed by units.

We notice that the processing energy and the energy consumed by units are neglected. Thus, we consider that the transmission energy presents the total of energy consumption.

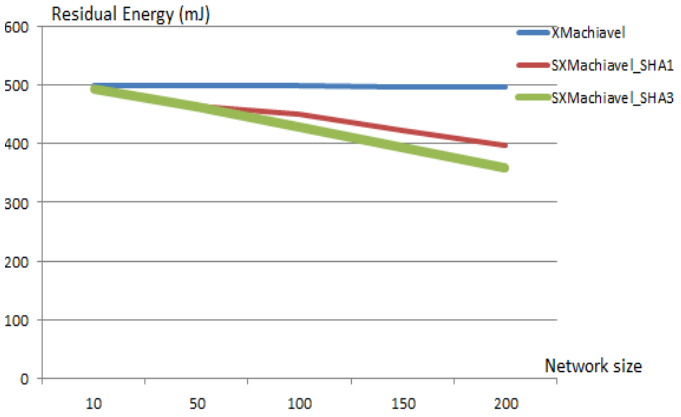

Figure 19**.**Variation of residual energy according to network size

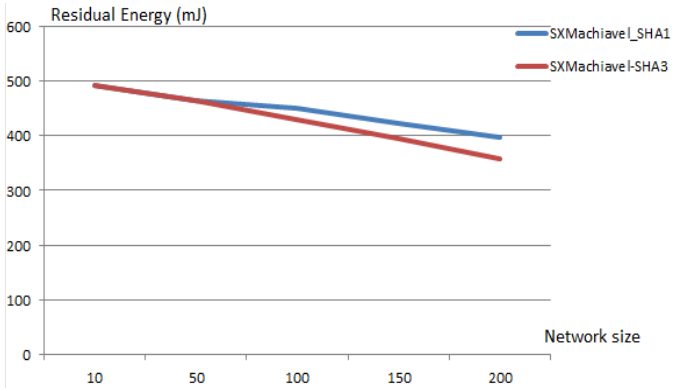

Figure 20**.**Variation of residual energy according to network size

Figures 19 and 20 show the variation of residual energy, according to the network size. According to these Figures, we notice that the existing non-secure protocol XMachiavel is less energy consuming; due to the absence of security mechanisms in this protocol. On the other hand, the energy consumption is higher for the case of SXMachiavel with SHA3; due to the addition of several security mechanisms which increase the total energy consumption, namely: an authentication mechanism, a hashing mechanism and an encryption mechanism. Consequently, it'spossible to exhaust the energetic resources of the nodes.

Unfortunately, there is always a trade-off between efficiency and energy consumption.

5. Conclusion

The implementation of a sensors network application must take into account the constraints that characterize the sensors nodes and differentiate them from other wireless networks types. These specifities, such as wireless communication-random deployment-resource limitation or unmonitored environment, have prompted the need to protect these networks by eliminating security vulnerabilities from the WSN.

The main challenges of our work are revealed in the cancelling at the security and energy conservation problems. These problems have required the emergence of numerous research studies proposed many solutions to ensure the reliability system, but it is based on the separation of both themes using either one or the other. Consequently, the originality of this work consists in combining the two features together (security and energy conservation) using a crossing between three layers: physical layer, data link layer and network layer. In the other hand and in our work, we have proposed a contribution which has consisted in using a cross layers security solution to obtain a secure-mobile network. This solution has started with the construction of a network deployment model specific to WSN. This model has consisted of sensors nodes partition in hierarchical areas; these areas are defined according to the radio range and the number of jumps. Then, this model can be generalized on any type of sensors (static, mobile or intelligent sensors that are differentiated from other sensors by adding the processor allowing data intelligent processing). Finally, we have secured this model. Stubborn that the proposed security solution has been appeared at: Firstly, in developing a new energy efficient and secure MAC protocol which provides a secure authentication- privacy & integrity. Secondly, implementing an intrusion detection system to protect the physical layer against jamming attacks. Simulations using OMNet++ take place to validate our solution and to estimate the performances of both protocols in terms of mobility rate, loss packets rate and energy consumption. The results showed that SXMachiavel is more successful in terms of mobility rate (can reach 99% compared with XMachiavel which doesn't exceed 33%), therefore and concerning the packets loss, the simulation result showed that it advances from 0.05% for a small network size. But, we deducted that the energy consumption increase by the addition of security techniques (residual energy decreases by 0.01% for each exchanged packet).

Acknowledgment

This work has been accomplished at WIMCS-Team research, ENET'COM, Sfax-University. Part of this work has been supported by MESRSTIC Scientific Research Group-Tunisia.

References

[1] M.Mezghani, R.Gatgout, G.Ellouze, A.Grati, I.Bouabidi, M.Abdellaoui, "Multitasks generic Plateform via WSN",International Journal of Computer Networks and Communications (IJCNC), vol.4, No.6, June 2011, pp.54-67. DOI: 10.5121/ijidps.2011.2406.

[2] Pr.M.M.Abdellaoui,''Multitasks-Generic-Intelligent-Efficiency-Secure WSNs and theirs Applications'', LAMBERT Academic Publishing (LAP), 2017, Part 3 : Secure Wireless Sensors Network, pp.142-185.

[3] S.Athmani, A.Bilami, "Protocole de sécurité pour les réseaux de capteurs sans fil", master memory, Hadj Lakhder-Batna University, Algeria, 15 juillet 2010, pp .1-96.

[4] Bouabidi Imen, Pr. Abdellaoui Mahmoud, ''Hierarchical organization by crossing between different layers for WSN energy saving'', International Conference on Advanced Technology & Sciences (ICAT'14), Antalya, Turkey , August 12-15 , 2014.

[5] Bouabidi Imen, Pr. Abdellaoui Mahmoud, ''Hierarchical organization by crossing between different layers for WSN energy saving'', 15th Internationnal conference on Sciences and Techniques of Automatic control & computer engineering-STA'2014, Tunisia, December 21-23 , 2014, pp.1-4.

[6] Bouabidi Imen, Pr. Abdellaoui Mahmoud, ''Hierarchical organization with a cross layers using smart sensors for intelligent cities'', SAI Intelligent Systems Conference, London, United Kingdom, November10-11 , 2015, pp. 446-451.

DOI: 978-1-4673-7606-8/15/$31.00 ©2015 IEEE.

[7] Bouabidi Imen, Pr. Abdellaoui Mahmoud, ''Energy Efficient Cross-layer MAC Protocol and Secure Authentication via an implementation of data confidentiality and integrity in WSN»,Future Technologies Conference 2016 (FTC), San Francisco, United States, December 6-7 , 2016. http://wwwpub.iaea.org/MTCD/publications/PDF/http://SAIconference.com/Conferences/FTC2016.

[8] V.Rajendram,K.Obraczka, J.J.Garcria-luma-Aceves, " Energy-Efficient, collision free Medium Access Control for Wireless Sensor Networks", Sensys'03, Los Angelos, California, USA, November 5-7, 2003, pp.1-12. DOI:1-58113-707-9/03/0011.

[9] S.Khatarkar, R. Kamble "Wireless Sensor Network MAC Protocol : SMAC and TMAC", Indian Journal of Computer Science and Engineering (IJCSE),vol.4, Aug-Sep 2013, pp.304 - 310.

DOI:ISSN: 0976-5166.

[10] B.Narain,et al,"Energy Efficient MAC Protocols for Wireless Sensor Networks: A survey", International Journal of Computer Science &Engineering Survey (IJCSES), vol.2, No.3, August 2011, pp.121-131.

DOI: 10.5121/ijcses.2011.2309.

[11] A.Warrier, J.Min, I.Rhee,''Z-MAC : a hybrid MAC for Wireless Sensor Networks'', pp.1-2.

http://conferences.sigcomm.org/sigcomm/2005/poster-123.pdf.

[12] C.Suh, Y. Ko and D.Son, " An Energy Efficient Cross-Layer MAC Protocol for Wireless Sensor Networks", Springer-Verlog Berlin Heidelberg, 2006, pp.410-419.

[13] A. Makke,''Détection d'attaques dans un systéme WBAN de surveillance médicale à distance'', phd diploma, Paris Descartes university, France, 30 May 2014, pp. 1-163.

[14] M.Rmayti, et al.,''Détection d'attaques Whormhole dans les réseaux MANETs en utilisant la théorie des graphes'', conference paper, december 2014,pp.1-16.

[15] L.B.Oliveira, et al., ''SecLEACH-A Random Key Distribution Solution for Securing Clustered Sensor Network'', FAPESP Under grant 2005/005579-9, pp.1-8.

http://www.cs.cmu.edu/~hcwong/Pdfs/secleach.pdf.

[16] A.N.Kulkarni, A.S.Tavildar,''Design and Performance Assessment for Energy Aware security Enhancing Strategy for PEGASIS protocol for MWSN'', International Conference on Information Processing (ICIP) Vishwakarna Institute of Technology'', December 16-19, 2015, pp.1-6.

[17] R.Singh, A.K.Verma,''Energy Efficient cross layer based adaptive threshold routing protocol for WSN'', International Journal of Electronics and communications-ELSEVIER, vol. 7 , February 2016, pp.166-173.

[18] U.Senthil Kumaran, P.Tlango, ''Secure authentication and integrity techniques for randomized secured routing in WSN'', Springer Science+Business Media Network, 27 August 2014, pp.1-9.

[19] S. Ghormare, V. Share,''Implementation of data confidentiality for providing High Security in Wireless Sensor Network'', IEEE Sponsored 2nd International Conference on Innovation in Information, Embedded and Communication Systems (ICIIECS), 2015, pp.1-5.
DOI: 978-1-4799-6899-6818-3/15/$31.00.

[20] P.Mohanty, M.R.Kabat, ''Energy Efficient structure-free data aggregation and delivery in WSN'', Egyptian Information Journals, ScienceDirect, vol.17, Issue 3, november 2016, pp.273-284.

[21] S. Misra , R. Singh, S. V. Rohith Mohan. "Information Warfare-Worthy Jamming Attack Detection Mechanism for Wireless Sensor Networks Using a Fuzzy Inference System", Sensors journal, 2010, pp. 3444-3479.

DOI:10.3390/s100403444.

[22] P.Inverardi, et al., ''Distributed IDSs enhacing Security in Mobile Wireless Sensor Networks'', Procceding of the 20th International Conference on Advanced Information Networking and Applications (AINA'06).
DOI: 1550-445X/06-$20.00, 2006, pp.1-5.

[23] D. E. Boubiche., ''Une approche inter-couches(Cross layer) pour la sécurité dans les RCSF'', PhD diploma in computer Sciences, Batna University, Algeria, pp.1-165.

[24] R. Kuntz,"Medium Access Control facing the dynamic of Wireless Sensor Networks", Phd diploma, University of Strasbourg, september 27 , 2010, pp.1-183.

[25] A. El-Hoiydi,''Spatial TDMA and CSMA with Preamble Sampling for Low power ad hoc wireless sensor networks'', 2007, pp.1-8.

http://www.mics.org/getDocum.pdf?docid=236&docnum=1.

[26] Best practices for EH&S software strategy planning, Verdantix, enablon, chapter1 Practice questions Mastering the Basis of security.

http://enablon.com/reports/best-practices-ehs-software-strategy-planning?campaign=G_D_Verdantix_New&gclid=CNa7ztXzxtECFU6dGwod43IMkg.

[27] H.Souilah, A.Baadache,''Coping with spoofed PS-Pool Based DOS Attack in IEEE 802.11 Networks'', pp.57-62.

http://ceur-ws.org/Vol-1256/paper5.pdf.

[28] https://en.wikipedia.org/wiki/SHA-3.

[29] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[30] F. Ahmed,''Strongest AES with SBox Bank and Dynamic key MDS Matrix (SDK-AES),''International Journal of computer and Communication Engineering, vol. 2, No. 4, July 2013, pp.1-5.

[31] S.J.Chang, el al.,''Third Round Report of the SHA3 cryptographic Hash Algorithm competition'', National Institute of standards and Technologiy, U.S.Departement of commerce, pp.1- 84.

[32] H. I.Reyes, N. Kaabouch, "Jamming and Lost Link Detection in Wireless Networks with Fuzzy Logic", International Journal of Scientific & Engineering Research , vol. 4, Issue 2, February 2013, pp.1-7.