International Journal of Advanced Research in Applied Science and Technology ISSN: 2456-1959
Vol.3, No.11, November 2017

Review on Attacks in Wireless Sensor Network

B.Vanitha M.Sc.,
Research Scholar (M.Phil.),
PG& Research Department of computer science,
Government Arts College (Autonomous)
Coimbatore-18
e-mail:vanithabathiran@gmail.com

Dr.M.Soranamageswari M.C.A., MPhil., Ph.D.,
Assistant Professor,
PG& Research Department of computer science,
Government Arts College (Autonomous)
Coimbatore – 18.
e-mail:sworanakannappan@rediff.com

ABSTRACT: Lately, wireless sensor network (WSNs) consume becomes an emerging technology and can be utilized in some circuital condition like battle grounds, commercial applications, environment observing, smart home, traffic surveillance and other different places. One of the foremost difficulties that WSN faces onwards is protection from serious attacks. The appearance of wireless sensor network (WSNs) can be considered one of the most important revolutions in the field of information and communications technology (ICT).Due to implementations of sensor networks in terms of many security attacks in such application layers. Wireless sensor networks (WSNs) area unit, severely anyone and area unit receptive malicious attacks.

Keywords: Wireless Sensor Network, Sensor Node, Attacks in (WNSs).

1. INTRODUCTION

The parallel evolution of micro technology, embedded systems and the field of global computing, many application continue to be designed in the field of wireless sensor networks. The sensor network mainly composed by four basic units sensing unit, the processing unit, the wireless transceiver unit and then power unit it also contain as domain applications. Supplementary modules such as a Global positioning system or energy generator system. Typically a wireless sensor network contains hundreds of thousands of sensor nodes. A sink or base station acts like an interface between users on the network .one can retrieve required information form the network by introducing data's and gathering results from the sink node. The individual nodes in a wireless sensor network are inherently resource constrained: they are limited processing speed, storage capacity, and communication bandwidth. This sensing technology is still in service today, albeit serving more peaceful functions of monitoring undersea wildlife and volcanic activity. The sensor can be deployed at various please with different usage and each have different capability to sense different attribute like temperature, moisture, pressure humidity etc. But these sensors have limited power source and also it is not cost effective to recharge the batteries. The batteries are usually exceptional [1].Therefore lifetime will depends on respective batteries of sensors the life of Wireless Sensor Network can be prolonged by using effective energy balancing methods.

Comparison of WSN with traditional wireless network:

1. Number of sensor nodes in WSN is much than any of traditional wireless networks
2. A major difference between WSN and other traditional networks computing devices including PC'S,PDA's and other embedded devices is that in WSN main emphasize is on power management.
3. WSN is data centric approach but traditional wireless sensor network are address centric because of large number of nodes in WSN [2].
4. Sensor nodes are much cheaper than nodes in other wireless networks
5. WSN use broadcast communication approach but traditional wireless network use point-to-point communication
6. Traditional wireless network like mobile ad-hoc network are designed for distributed computing while WSN are designed to gather information.
7. A unique characteristic of WSN is that data collected by adjacent nodes and some consecutive readings sensed by sensor are highly correlated which give opportunity to develop efficient protocols.
8. MAC in traditional wireless networks consumes 2-6 time more energy than S-MAC for traffic load with message sent every 1-10s.

1.1. WIRELESS SENSOR NETWORK COMMUNICATION ARCHITECTURE:

WSN architecture includes both a hardware platform and operating system designed, Tiny OS is a components based operating system designed to run in resource constraint wireless device.

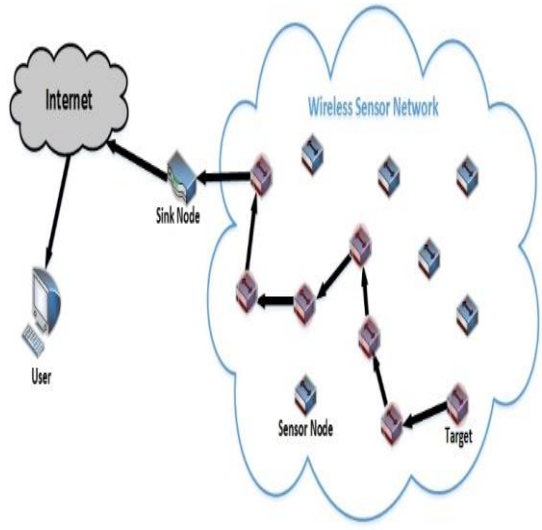

fig1: WSN Communication Architecture

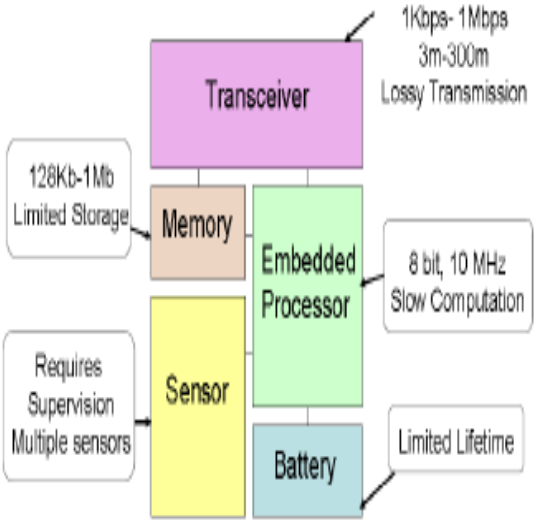

Fig2: Main basic units of a sensor node

The communication of WSN are:

- **Sensor field**: The area in which sensor nodes are deployed.
- **Sensor Nodes**: Sensor nodes are the sensors which are responsible for gather information and routing this information back to sink.
- **Sink**: It is also a sensor node which performs a special task of receiving, processing and strong data form other sensor nodes. This node is responsible for reduction of message need to be sent and also reduce the energy requirements [3].
- **Task Manager (Base Station)**: It is a centralized point of control within the network used to extract information form the network and passes control information back to the network.

1.2. ARCHITECTURE OF WIELESS SENSOR NETWORK NODE

A sensor is a tiny device which is based on micro sensor technologies with low signal processing capability, low computation power and low bandwidth.
Mani Component of wireless sensor node [4].

- Sensor unit
- Processing unit
- Radio Trans receiver
- Battery

1.4. PROTOCOL STACK OF WSN

- **Application layer:** there possible application layer protocols.ie.., Sensor Management Protocol (SMP) Task Assignment And Data Advertisement Protocol(TADAP) and Sensor Query And Data Dissemination Protocol (SQDDP), [5]needed for sensor network based on the proposed schema's related to the other layer and sensor network application.

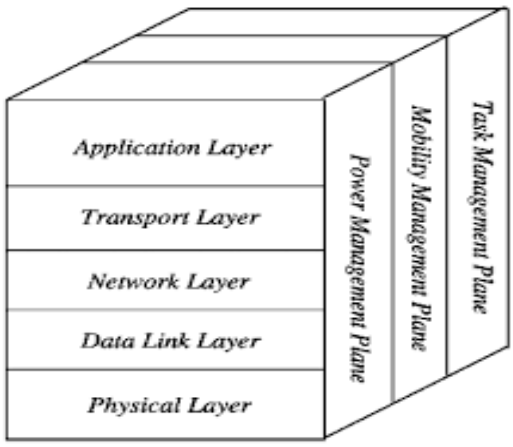

Fig3: protocol stack of WSNs

- **Transport Layer:** It provides communication of network which outside world.
- **Network Layer:** Like traditional networking with external networks.

- **Data Link Layer:** Like traditional network's data link layer it provide multiplexing of data streams, medium access and error control
- **Physical Layer:** It is responsible for frequency selection, signal detection, encryption and modulation. This layer modulation. This layer also minimizing the energy.

Layering approach in sensor network attacks and countermeasures:

- The attacks and countermeasures in a layer model in sensor networks.

Layer	Attack type	Countermeasures
Application Layer	Subversion and Malicious Nodes	Malicious Node Detection and Isolation
Network Layer	Wormholes, Sinkholes, Sybil,blackhole, Routing loops	Key Management, Secure Routing
Data Link Layer	Link layer Jamming	Link layer encryption
Physical Layer	DoS and Node capture attacks	Adaptive antennas, Spread Spectrum

Table 1: Sensor Network Attacks Type

2. SECURITY GOLS WIRELESS SENSOR NETWORKS:

Security goals in sensor networks depend on the need to know what we are going to protect. Two type of security goals. There are: (I) Primary Security Goals (ii) Secondary Security Goals [6].

I. Primary security goals:

- Primary security goals in sensor networks which are Confidentiality, Integrity, Authentication and Availability (CIAA).
- A malicious node present in the network injects false data.[7]
- Unstable conditions due to wireless channel cause damage or cross data.

- **Confidentiality***:*

  The ability to conceal message from a passive attacker, where the message communicated on sensor networks remain confidential.

- **Integrity:**

  The ability to confirm the message has not been tampered, altered or changed while it was on the network.

- **Authentication:**

  Need to know if the messages are from the node it claims to be from, determining the reliability of message's origin.

- **Availability laity:**

  It's determine if a node has the ability to use the resources and the network is available for the messages to move on. [8]

II. Secondary Security Goals:

Secondary security goals in sensor network which are data freshness, authentication, and authorization secure localizations

- **Data freshness:**

In sensor networks, the transmitted data are often derived from regularly repeated measurements. Therefore, it is essential to be able to ensure that information is recent or not in order to guarantee the reliability of WSN applications. Then data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages. [9]The data freshness is a security criterion which helps to fight against replay attacks.

- **Authorization:**

Authorization is the function that specifies access rights to resources. Authentication and authorization should not be confused because they are two different processes. After authentication, the authorization determines the access rights of the authenticated system to the accessed objects. Then, the authorization techniques ensure that only authorized entities communicates across the network.

In the WSN infrastructure, only communications between legitimate entities (nodes and users) must be permitted. It is important to ensure that network access is only possible for the authorized nodes, and also for the users which only have the required rights. Consequently, authorization mechanisms are also intended to block unauthorized access to the network [10].

3. ATTACKS IN WIRELESS SENSOR NETWORKS:

In this section we describe a non-exhaustive but representative list of the most common and known attacks in WSNs, which can be classified in two main categories: passive or active attacks.

A passive attack is one in which the intruder eavesdrops but does not modify the message stream in any way. An active attack is one in which the intruder may transmit messages, replay old messages, modify messages in transit, or delete selected messages from the wire. [11]

A. Passive listening or eavesdropping

This attack consists of listening without altering the data or the operation of the network. It is generally undetectable but prevention is possible. Also called eavesdropping, it is a network layer attack that focuses only on capturing packets transmitted from the network by other nodes and reading the data content in search of any type of information. This type of network attack is generally one of the most effective as a lack of encryption services is used.

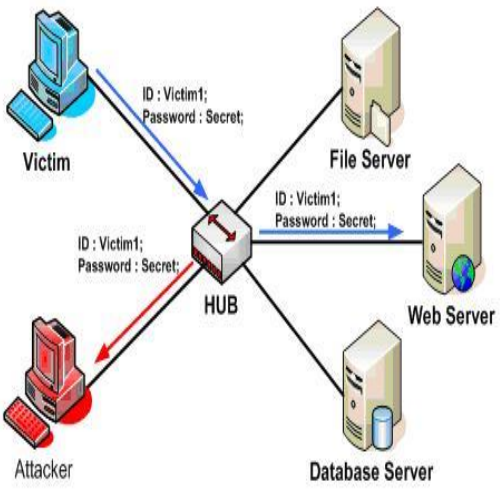

Fig4: Passive listening or eavesdropping

B. Traffic analysis

The attacker analyses the paths taken by the packets to recover valuable information about the vulnerabilities of the network. Traffic analysis can allow an attacker to know the location of base stations or data aggregation nodes by locating locations where the greatest number of packets pass through.

C. Man-in-the-Middle Attack

A Man-in-the-Middle attack is an attack in which the attacker intercepts information ex-changed between two nodes. The two legitimate nodes think they are communicating directly with each other and do not suspect the presence of the intruder. [12]

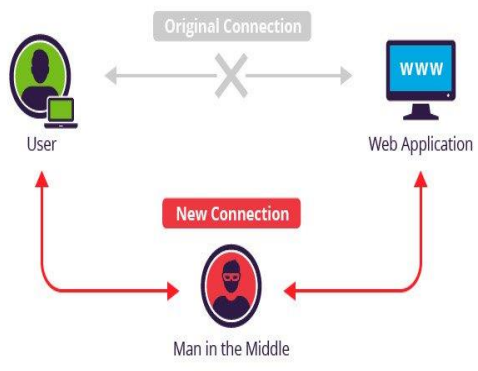

Fig5: Man-in-the-Middle Attack

This one could create and control a communication channel to eavesdrop, analyse traffic, insert, and block arbitrary messages within it.

D. Hello flood attack

An attacker performs a hello flood attack by broadcasting Hello messages on reaching certain network nodes which in turn will try to join the striker who is actually out of range.

A repetition of such an attack would reduce energy nodes that will be forced to unnecessarily respond to every request of the attacker.

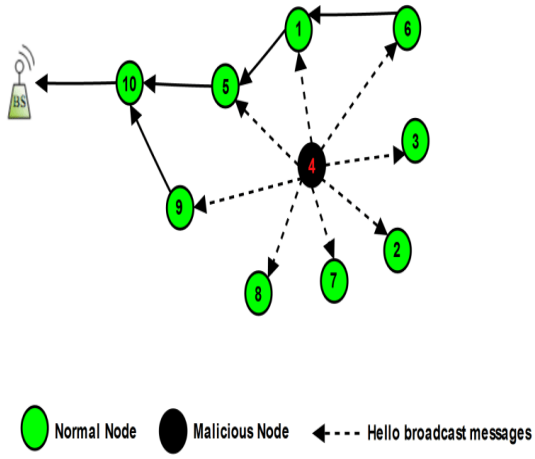

Fig5: Hello flood attack

E. Flooding

In this type of attack, [13] an attacker uses one or more malicious nodes or a particular device which, in some cases, has strong transmission power, to regularly send messages on the network in order to saturate it.

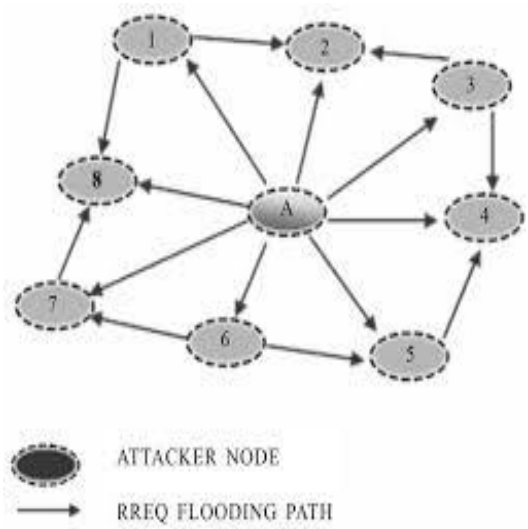

Fig6: Flooding

This is an active attack that is of the same type as denial-of-service attacks in conventional networks.

F. Replay attack

In a replay attack, an attacker intercepts the packets of a valid session and then replays they later. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. To illustrate this attack, one can consider as an example a sensor network designed for fire detection purpose: if a first case of fire is detected and then a sensor node sends an alert packet to inform the control centre, the attacker can register this packet, even if it is encrypted, and then retransmits it later. This will cause a new fire detection alert different from the first one. This attack is possible if the packet does not contain information concerning the sending date and time or if this date is accessible and easily modifiable by an attacker. [14]

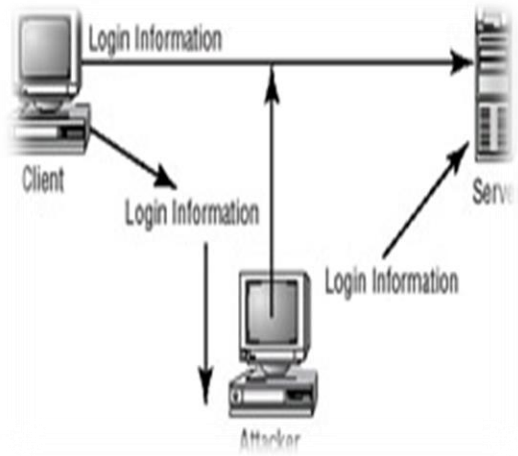

Fig 7: Replay Attack

G. Message insertion

The attacker seeks in various ways (using malicious nodes, sending packets on the same radio frequency, etc.) to insert messages into the network traffic. [15]This attack makes it possible to saturate, disrupt the network, or to deceive it by sending false information.

H. Message alteration

A malicious node will retrieve a message and alter it,adding false information (about the recipient, thesender, the information itself) or modifying it.

I. Byzantine attack

The Byzantine attack is described in a WSN designed for the task of distributed binary detection. Their network consists of n sensors, each making an independent and identically distributed observation about the State of the Nature (said H1 or H0).These observations are successively delivered to a common fusion centre for the final decision on the underlying statistical hypothesis. In a Byzantine attack, malicious nodes which are referred to as the Byzantines sensors will cooperatively works against the network by delivering data according to certain fictitious distributions properly designed in order to impair the detection capability of the fusion centre.

J. Wormhole attack

The wormhole attack is an attack in which an attacker intercepts packets in one location and forwards them to another location of the network. With this attack in the network, non-neighbouring nodes may believe they are neighbours, which somewhat disturbing routing and clustering operations.

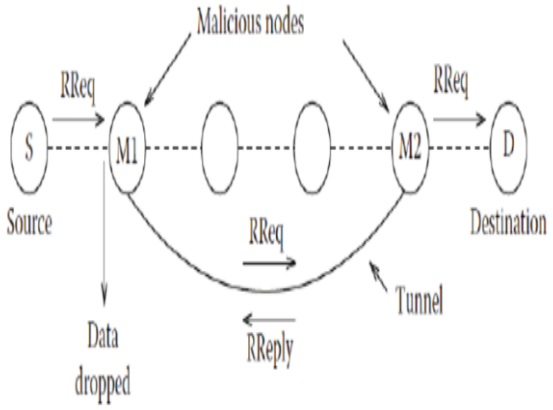

Fig6: Wormhole attack

K. Sybil attack

In a Sybil attack, a malicious node holds simultaneously multiples identities in the network. This type of attack can affect the clustering operations by choosing a bad cluster head or the aggregation by distorting aggregation results.

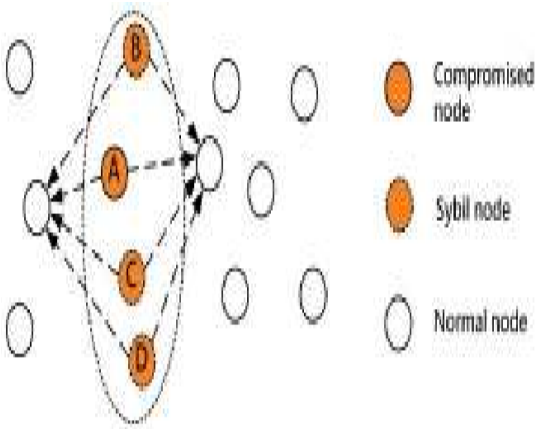

Fig7: Sybil attack

L. Sinkhole attack

In a sinkhole attack, an attacker compromises a node and manages to make it attractive against other nodes. With this attack, the normal nodes can for each operation, send data to the malicious node. The sinkhole attack is a particularly severe attack which prevents the base station from obtaining complete and correct sensing data.

M. Black hole attack

In wireless sensor networking, black hole attack refers to introduce malicious nodes in the locations where incoming or outgoing traffic could be silently discarded or dropped, without informing the source that the data did not reach its intended recipient. In a black hole attack, the black hole nodes themselves are often invisible, and could be detected by monitoring the lost traffic.

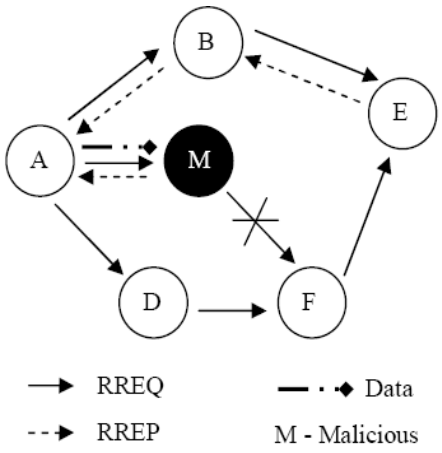

Fig7: Black hole attack

N. Gary hole or selective forwarding attack

In this type of attack, an attacker can compromise a node which could choose to forward messages or not. In the gray hole attack the malicious node could act as a normal node and then choose to drop some messages which are passing through it, while transmitting other packets.

In this case, important messages might not reach their final destinations. This type of attack can disrupt the normal operation of applications and cause a possible denial of service (Do's).

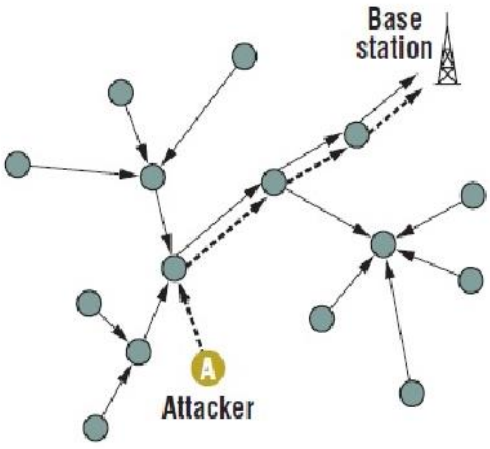

Fig8: Selective forwarding attack

O. Node Capture Attack

Most WSNs are often deployed in hostile areas that do not allow human monitoring of all sensors. It is then quite possible for an attacker to compromise a sensor. This node controlled by the attacker will allow him to access the network to retrieve sensitive information or to launch other attacks from this node. Thus, in Node Capture Attack, an attacker physically takes control of a sensor node and then compromises it so that stored data become inaccurate or manipulated. Capturing a node enables an adversary not only to get a hold of cryptographic keys and protocol states, but also to clone and redeploy malicious nodes in the network.

P. Sensor type specific attack

In this type of attack, an attacker modifies the physical behaviour of the sensor. For instance, he can light a flame in front of a thermal sensor or light a lamp in front of a light sensor to deceive sensing operation. For this purpose, the compromised node will constantly send alert or continue recording false information until its energy is exhausted.

Q. Jamming attack

In a jamming attack an attacker sends a powerful radio signal that will interfere with the sensor signals in order to disrupt legitimate communications and then cause a Do's attack.

There are many other possible attacks in sensor networks, including attacks related to the top layer of TCP/IP applications such as repudiation, data corruption, hijacking session, SYN flooding, location disclosure attacks, Do's, impersonation, cryptographic primitive attacks, etc. As we can see, WSN security remains a real challenge sometimes due to the nature of deployment and sensors constraints. Several security techniques are proposed, but it should be noted that some of them are inappropriate. On the other hand, others seem well suited to sensors.

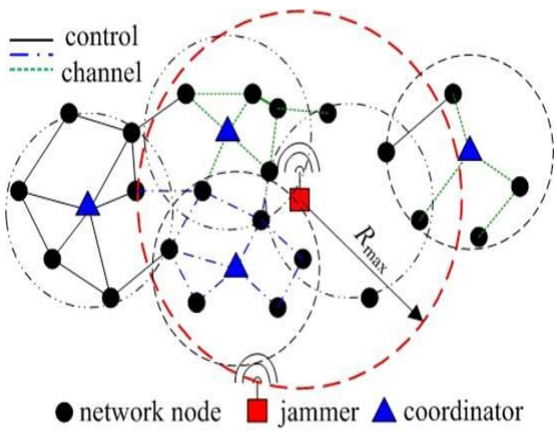

Fig9: Jamming attack

4. CONCLUSION

Wireless sensor network has a remarkable feature to monitor environmental and physical conditions. In this paper various aspects of wireless sensor networks and various type of WSNs layer of attacks are discussed. How it is differ from traditional wireless networks, and then security goals in WSNS,

Wireless sensor network has bright future in the field of networking because it continuingly providing us solutions for many security attacks. Also it conclude that to make the wireless sensor network secured in network layer attack in the larger area for future work.

REFERENCES:

[1] K. Lama, M.Hamraoui, H.Belhadaoui. "Study of the credibility of the information shared by a wireless sensor network." 2015 5th World Congress on Information and Communication Technologies (WICT), (pp. 113-116). IEEE.

[2] K.Lahma, M.Hamraoui, H.Belhadaoui, A.Mektoubi, "Indice de crédibilité d'un noeud capteur dans un réseau de capteurs sans fil" CMT-2016 Mai 2016, Tetouan, Maroc.

[3] C.T.KONE, "Conception de l'architecture d'un réseau de capteurs sans fil de grande dimension, Université Henri Poincaré, Nancy I, pp. 17-19.

[4] A.J.G.Sanchez, "Wireless sensor network deployment for integrating video-surveillance and data-monitoring in precision agriculture over distributed crops", Computers and Electronics in Agriculture 75 (2011) 288–303.

[5] E.Hamida. "Modélisation stochastique et simulation des réseaux sans fil multi-sauts. " L'Institut National des Sciences Appliquées de Lyon, 2009.

[6] D.Curiac, C.Volosens, "Redundancy and Its Applications in Wireless Sensor Networks: A Survey. Transactions on computers", April 2009, New York, USA,pp.705-714.

[7] L.Khelladi, N.Badache "Les réseaux de capteurs : état de l'art. " Laboratoire des Logiciels de Base, CERIST, Fevrier 2004.

[8] S.Nadir, A. Marzak, K. Lahma, H. Belhadaoui, M. Hamraoui, "Communication protocolaire hybride des données massives distribuées traitant en parallèle la crédibilité de l'information: Application au WSN "WCMCS 2014, August 9-11, Hammamet, Tunisie.

[9] S.Nadir, A. Marzak, K. Lahma, H. Belhadaoui, M. Hamraoui, "Design and complexity analysis of algorithm treating the credibility of the information: Application to WSN" NNGT Int. J.on Networking and Computing, Vol.2, Feb 2015.

[10] E.Rahm and H.H. Do, "Data Cleaning: Problems and Current Approaches," IEEE Data Eng. Bull., vol. 23, no. 4, pp. 3-13, Dec. 2000.

[11] E.Elnahrawy, B.Nath, "Cleaning and querying noisy sensors", WSNA 03 Second ACM International Workshop on Wireless Sensor Networks and Applications, San Diego, CA, USA,Sep2003.

[12] S.R.Jeffery, G.Alonso, M.J.Franklin, W.Hong. and J.Widom,"A pipelined framework for online cleaning of sensor data streams".In Proceedings of the 22nd International Conference on Data Engineering, April 2006.

[13] D.Hamdan. "Détection et diagnostic des fautes dans des systèmes à base de réseaux de capteurs sans fils." LASTRE, Avril 2013, pp.66-69.

[14] P.Dusart, "Cours de statistiques inférentielles", 2014, pp.27-30.

[15] Saporta, G.(2011). "Probabilités, analyse des données et statistique",Editions Technip.pp.574-576.