ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 6, 229-243 (2019)

www.astesj.com

Special Issue on Multidisciplinary Sciences and Engineering

ASTESJ

ISSN: 2415-6698

Attacks classification and security mechanisms in Wireless Sensor Networks

Amine Kardi[1,*], Rachid Zagrouba[2]

[1]*Faculty of Mathematical, Physical and Natural Sciences of Tunis, University of Tunis El Manar, 2092 El Manar, Tunisia*

[2]*College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia*

A R T I C L E I N F O

Article history:
Received: 12 September, 2019
Accepted: 16 November, 2019
Online: 05 December, 2019

Keywords:
Wireless Sensor Networks
Routing attacks
Cryptography
Security
NS3 simulator

A B S T R A C T

This paper proposes a new classification model distinguishing four classes of attacks in Wireless Sensor Networks (WSNs) namely: attacks based on the protocol stack, on the capability of the attacker, on the attack impacts and on the attack target. Then, it presents and classifies the most known attacks in WSNs based the proposed model. Simulations implemented under the NS3 simulator prove that the network lifetime can decrease by more than 45% in the presence of attacks. Afterwards, it discusses the main security methods and protocols of management and distribution of encryption keys used to ward off different types of attacks. Obtained results confirm that these security methods must be adapted to the specific characteristics of WSNs to achieve the intended objectives.

1. Introduction

With the widespread use of WSNs[1][2], composed of a small and low-powered communicating devices usually deployed in hostile environments, and due to their resources constraints, security factors become crucial and challenging with the appearance of a variety of attacks targeting these networks [3][4][5]. The main contribution of this paper is to provide a survey of these attacks and of the security techniques which will facilitate the design of WSNs for researchers and routing protocol programmers.

The rest of the paper is organized as follows: Security requirements for WSNs are discussed in Section 2. Section 3 introduces our proposed taxonomy and discusses each category of attacks. Section 4 presents the main attacks in WSNs and analyzes them using NS3 simulator. The basic security mechanisms in WSNs are presented in Section 5 then followed by the analysis and findings in section 6. Lastly; we conclude the paper and highlight our future work in section 7.

2. Security requirements for WSNs

Due to the lack of a wired communication medium, the limited resources of sensors and the properties of the deployment [6][7], WSNs, deployed mostly in hostile environments with mission-critical tasks, have several security challenges which are more complex than with other types of networks. As an ad hoc network, security requirements for WSNs include the standard security metrics known as CIAA (Confidentiality, Integrity, Authentication and Availability) in addition to the security requirements specific to this type of network which aim to protect the information and resources from attacks and misbehavior. In the following we discuss the security properties and requirements we would like to achieve in order to establish a reliable communication in WSNs and to provide secure services [8].

2.1. *Standard security requirements*

As with other types of networks, standard security requirements are needed in WSNs such as:

- **Confidentiality:** This is the most important issue in network security which guards data from eavesdroppers. It ensures that a given message remains hidden and cannot be used by anyone other than the desired receiver. It protects packets from undertaking traffic analysis, passive attackers and modification. The standard approach for achieving this requires use of encryption techniques [9].
- **Integrity:** Data integrity is needed to ensure the reliability of data parquets. In fact, sent packets must be protected from modification (adding, altering, deleting, damaging or losing) by malicious intermediate nodes or by wireless channel disturbance during the transmission [10].

*Amine Kardi, Tunis, (+216.96.27.90.33),Email : amine.kardi@fst.utm.tn

- **Authentication:** all applications require data authentication which ensures the reliability of the message by giving the ability of each communication host to identify its origin and to verify the other's identity to counter to packet injection or spoofing and to all malicious routing information. Critical characteristics of sensor nodes and the wireless nature of the communication medium in WSNs make extremely challenging to ensure authentication in these networks [11].
- **Availability:** Availability affects several sides in the sensor network. In fact, it determines whether a node can use the resources if needed, whether data and services are available for on-demand use and whether the network is always available to ensure communication even in the presence of malicious attacks. A loss of availability may have serious impacts and threat the entire network, e.g. it may open a backdoor for malicious invasion in some cases and sensed information may become useless or of lower value, but also providing availability can hurt the network lifetime especially with limited energy resources [12].

2.2. *Specific security requirements*

Node characteristics and deployment environments make WSNs vulnerable to special attacks and subsequently several security requirements specific to this type of networks are needed such as:

- **Authorization:** ensures that only authorized nodes can manipulate data (provide, update...) in the network and prevents unauthorized access to resources [13].
- **Nonrepudiation:** it prevents a node from denying sending a message it has previously sent through the network [14].
- **Data freshness:** implies that used data are recent and valuable and cannot be replayed by a malicious actor, under any circumstances, after abandonment to prevent, i.e. overloading the network by sending previously captured packets. Timestamps and time-related counters can be used to ensure data freshness [15].
- **Transparency:** after leaving the network a sensor node should not be able to replay old packets or to read any future messages in the same way as a joining node should not be able to reload or to read any previously transmitted message in order to protect the network from malicious injected nodes [16].
- **Self-Organization:** In the absence of an overall network management infrastructure, sensor nodes which have the ability of self- organization may encounter several hazards and risks threatening the safety and operation of the entire network [17].

  Time Synchronization: due to its limited energy resources, sensor nodes may be turned off for periods of time in the form of a smart sleep in order to conserve energy and, in some application, the end-to-end delay of some packets is of a great extent that is why collaborative sensor nodes require a synchronization system which must be ensured by a secure synchronization protocol to deal with attacks that attempt to affect proper synchronization between nodes [18].
- **Secure Localization:** In several applications, sensor networks are designed to locate faults. Consequently, the network must be able to accurately and automatically locate each sensor node that is why location information must be handled in a secure manner to avoid attacks taking advantage of the security weaknesses of this information [19].
- **Anonymity:** malicious actors do not have to decrypt the source node of a packet in order to secure nodes and the sensing area which can be affected by erroneous data [20].
- **Survivability:** Network services and functionalities must be maintained even with the low levels required in the case of failures, attacks and compromised or destroyed nodes [21].

According to these security requirements, it's obvious that attacks in WSNs can be of different types and can affect the entire network system such as nodes, packets, data, paths, routing etc. The following section presents our proposed taxonomy.

3. Taxonomy of attacks in WSNs

Because of its specific characteristics, WSNs are vulnerable to various types of attacks. These attacks are of different mechanisms, techniques and goals which makes necessary to find and adopt a well-defined taxonomy in order to facilitate design and development of WSNs for researchers and protocol programmers.

According to the security requirements mentioned above, and taking into account the mechanisms and parameters of attacks; we propose a new taxonomy which divides attacks in WSNs into four major classes namely: **attacks based on the protocol stack, based on the capability of the attacker, based on the attack impacts and based on the attack target** as shown in figure 1.

A detail overview of each security attack class is discussed in the rest of this section.

3.1. *Attacks based on protocol stack*

The protocol stack used by nodes in a wireless sensor network consists of the Physical Layer, Data Link Layer, Network Layer, Transport Layer, Application Layer, power management plane, mobility management plane and task management plane as shown in figure 2. It ensures the energy efficiency in the network, manages the use of the wireless medium with the routing task and facilitates synchronization and cooperative efforts between sensor nodes.

Each level on the protocol stack takes on a set of tasks and guarantees a set of services. Therefore, it will be targeted by several attacks.

- Physical Layer:

This layer ensures the data transmission services which encompass the selection of access channels, radiofrequency regulation and deflection, signal processing and data encryption to increase the communications reliability. The importance of this layer exposes it to a variety of attacks targeting data privacy, resource depletion, signal and communications interruption, and so on [22].

- Data Link Layer:

This layer is responsible of physical addressing, error detection and/or correction, data streams multiplexing, medium access and

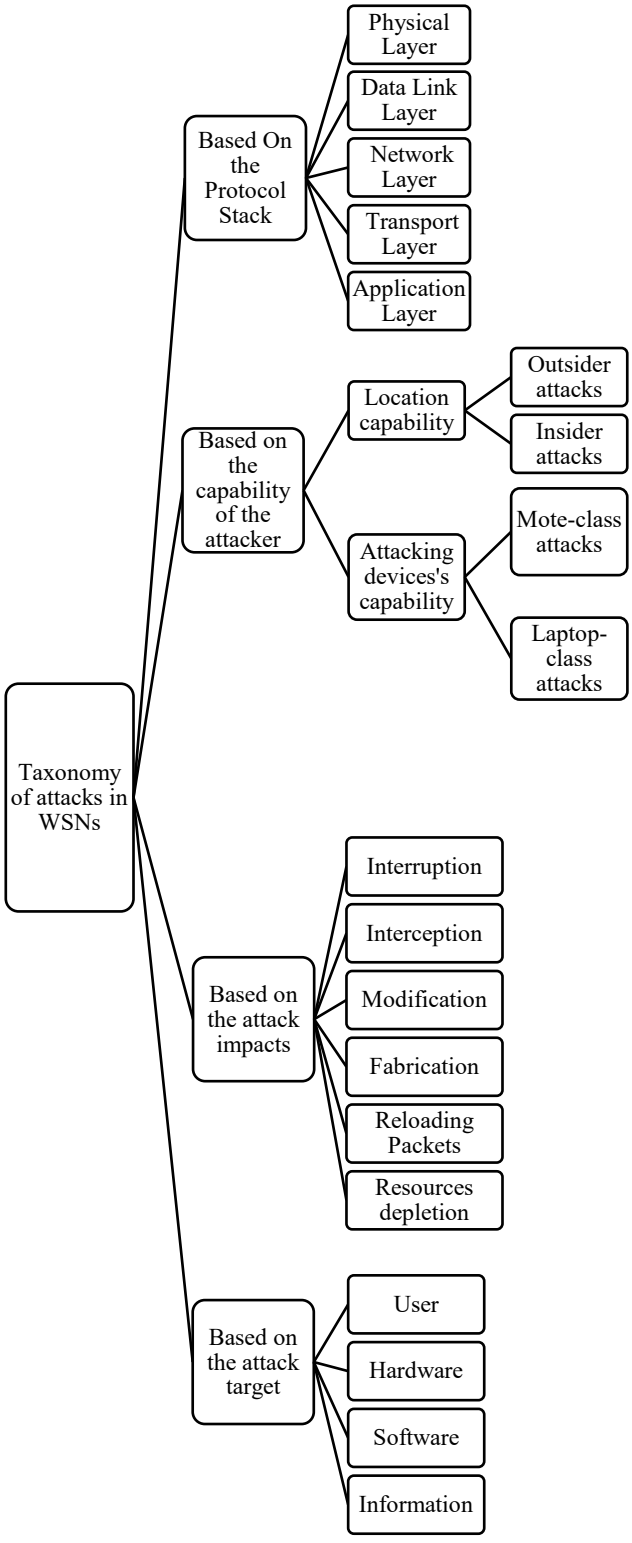

Figure 1: Security attacks in WSNs: A taxonomy

flow control as well as ensuring reliable point-to-point and point-to-multipoint connections in the network. The medium access control (MAC) protocol must support mobility and be able to handle collisions and to achieve energy efficiency in the network. The importance of this layer makes it vulnerable to several types of attacks sources of collisions, resource exhaustion, and network destruction [23].

- Network Layer:

This layer is in charge of routing the data supplied by its upper layer. It is very important task encompasses packets routing and forwarding, addresses assignment and energy management. These axial and fundamental tasks attract several attacks aimed at absorbing the network traffic, disrupting communication, exhausting resources, intercepting paths and injecting malicious packets [24].

- Transport Layer:

The transport layer ensures the management of end-to-end reliable delivery of packets connections and the establishment of end-to-end connection in addition to flow and congestion control. It is especially needed when the system is planned to communicate with external networks. Several attacks target this layer in order to reduce the network's availability, to degrade or even prevent data exchange and to waste energy [25].

- Application Layer:

This layer contains user applications which oversee the sensing tasks. It manipulates user data with a set of application protocols, and it is a target of attacks aiming at affecting the synchronization of communications and data confidentiality.

The power management plane and the mobility management plane are responsible, respectively, for the management of energy resources and the mobility of nodes in order to achieve maximum energy efficiency and stability of communications. The task management plane manages the sensing tasks and ensures synchronization between sensor nodes [26].

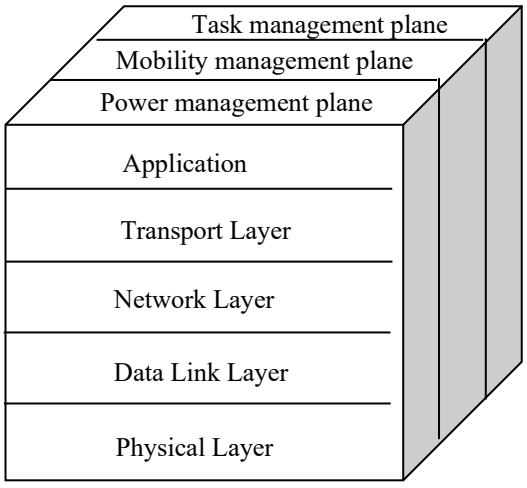

Figure 2: The protocol stack of sensor networks

3.2. *Attacks based on the capability of the attacker*

Based on the capability of the attacker, attacks in WSNs can be subdivided into two classes: Location capability and Attacking

device's capability. Each of these classes is further divided into two broad subclasses according to the relative capabilities of the attacker which are respectively: Outsider/ Insider attacks and Mote-class/ Laptop-class attacks. In the following we detail each of these subclasses.

- Outsider/ insider attacks

Based on the location capability of attackers, attacks in WSNs can be classified into Insider and Outsider attacks. We are talking about insider attacks when a legitimate nodes belonging to the network and which are actually part of it are compromised and participates in unintended and/or unauthorized ways in the attack contrary to outsider attacks which are launched only from outside the networks application environment and performed by external nodes which do not belong to the WSN. Insider attacks are more severe when compared with outside attacks since compromised nodes contains secret information and may not be detected due to the possesses privileged access rights they had. These attacks target the entire network and affect the resources, data, communications and even the existence of the network. Some papers refer to internal and external attacks [27].

- Mote-class/ laptop-class attacks

Based on the Attacking device's capability, attacks in WSNs can be classified into Mote-class and laptop-class attacks. In mote-class attacks, attackers use malicious nodes with similar techniques capabilities and hardware proprieties to the network nodes in order to execute malicious codes aiming to affect the network functionalities (data, routing, paths, energy management...). Contrariwise, attackers use more powerful devices with great transmission range, processing power, and energy supply than the network's sensor nodes in laptop-class attacks e.g., a laptop which results in launching more serious attacks and consequently lead to more serious damage to the target network [28].

3.3. *Attacks based on the attack impacts*

Based on the attack impacts, attacks in WSNs can be subdivided into six classes: Interruption, Interception, Modification, Fabrication, Reloading Packets and Resources depletion. In the following we detail each of these four classes.

- Interruption

The attacker aims, through some techniques, to interrupt the network's functionalities. These attacks are varied and can target nodes, sinks, paths, routing task, resources depletion etc. which threaten services availability. Even in the presence of an attack, the network must be capable of maintaining its functionalities without interruption [29].

- Interception

These attacks are used when the attacker intended to eavesdrop on the network information. This threatens message confidentiality, network services availability and may result in the depletion of resources [30].

- Modification

These attacks threaten data integrity. Attackers intend to eavesdrop to information and to tamper with it in various ways: Injection, removal, modification etc. in order to disrupt the network functionalities and threaten the accuracy of services and treatments [31].

- Fabrication

These attacks are manifested by the injection of erroneous data into the WSN. Attacker aims to threaten message authenticity and network availability through the depletion of the energy resources of the network especially with wireless communications which are very energy intensive [32].

- Reloading Packets

In some cases, the attacker seeks to reload and read previously transmitted packets from a compromised node or from buffers of active nodes which threatens data confidentiality and packets transparency. These packets can be injected back into the network, which threatens messages freshness and wastes energy [33].

- Resources depletion

In a WSN, resources depletion leads to the complete collapse of the network. Attackers aim to waste limited energy resources of nodes using various processing and transmission tasks [34].

3.4. *Attacks based on the attack target*

Attacks in a WSN can target different actors and components of the network which are users, hardware, software and information [35]. In the following we detail each of these targets.

- User

Various users of a WSN like humans, robots etc. can be targeted by malicious attacks aiming to have an authorized access to the network system through legitimate compromised identifiers. These attacks seek to take control of the network, to use it for personal tasks, to use information or to destroy it.

- Hardware

Attacks targeting hardware in WSNs tend to compromise nodes for malicious intent, waste limited energy resources or destroy equipment. A compromised node may contain secret information and may be used for unauthorized access to the network.

- Software

Attacks targeting software in WSNs aim to eavesdrop information, control the network and disrupt the services and functionalities.

- Information

Attacks targeting information in WSNs are various e.g. the attacker can falsify the data supposed to be sensed in the sensing area, in other cases, sensed data can be targeted by attacks, packets in transit, authentication parameters etc. Attackers aim at affecting the network functionalities, services availability and data confidentiality.

Each of these classes helps to analyze and study attacks in WSNs from different perspectives. We detail, in the following section, the most known attacks and countermeasures to counter their effects.

4. Attacks in WSNs

Generally, attacks under these four classes, can be either active or passive. A passive attack is an attack that aims to gets exchanged

data in the network without interrupting the communication to remains hidden and not be discovered. Passive attackers listen and collect data that can be used later to start other types of attacks. While active attacks involve some modifications in the data stream. In fact, it seeks to modify, fabricate, inject a false stream or intercept the data or the communication to disrupt the normal functionality of the network. In the active mode the attacker is more aggressive and aims to damage the entire network [36].

4.1. *The most known attacks:*

Among the most known attacks in WSNs we find:

- Jamming:

Jamming attack [37] takes advantages of the sensitivity of the wireless medium to interferences and results in a denial of service in the network. Attacker identifies the radio frequencies used by the targeted WSN and tries to disrupt or block communications by emitting signals (unnecessary information) in the same frequencies that inhibit communication (messages transmission and/or reception) between nodes. This interference may be temporary, intermittent or permanent and can affect all or part of the network depending on the radio range of the jamming source which can have the same characteristics as the network nodes as it can be more powerful. Jamming can be of different types: it can be constant if it targets and corrupts data packets in transit, deceptive when sending a constant data stream in the network, random when injected data streams are dispersed over time and reactive if the jamming source sends a jam signal following the detection of traffic. Jamming can target different layers: It can interfere with radio frequency signals at the physical layer, as it can take advantages of the medium access control protocol causing malicious collisions at the link layer as it can target the network layer by injecting malicious packets. Defense techniques [38][39][40] against Jamming attack involve spread-spectrum techniques for radio communication such as frequency hopping to switch between many frequency channels, authentication mechanisms to detect malicious and replayed packets, the use of secure medium access control protocols etc.

- Tampering or destruction [41]:

WSNs are highly vulnerable to physical attacks as they are often deployed in unprotected areas. A Tampering attack will be triggered after physically capturing the node and aims to retrieve cryptographic material as encryption keys and the program code stored within a node which can be used later to trigger other types of attacks such as modifying routing information, creating duplicate data packets, tampering routing services etc. or to manipulate the captured node by installing a new code causing an abnormal behavior of the compromised sensor, controlled by the attacker, in order to disrupt the network. Destruction attack consists of removing the sensor from the network by destroying it resulting in isolated areas and even the destruction of the entire network. Defense techniques against this attack are based on the principle of considering the situation in which sensor nodes are compromised such as tamper-proofing the physical package of nodes.

- Continuous Channel Access (Exhaustion):

Exhaustion [42] belongs to DoS attacks. It aims to exhaust the batteries of the nodes in order to reduce the network lifetime. It consists to disrupt the Media Access Control protocol, by continuously injecting unnecessary packets in the network and requesting or transmitting data over the channel entail the waste of node energy in unnecessary retransmissions. A possible solution to this attack is the Rate Limiting at the MAC admission control which allows ignoring corrupted packets and excessive malicious requests [43] [44].

- Collision:

Collision attack [45], similar to the continuous channel attack, can be caused by malicious nodes by transmitting packets in the network in order to block / delay the communication between nodes which results, in addition to the throughput, in a waste of energy and a loss of data. It is difficult to detect Collision attack in WSNs because it is a short time attack using malicious packets which are similar to legitimate packets. Researches, such as [46], proposed several Collision detection techniques such as error-correcting codes.

- Unfairness:

Unfairness attack [47] is a partial or a weak form of DOS attack that can result in marginal performance degradation. Based on other attacks such as collision and exhaustion, collision attack decreases significantly the utility and efficiency of services. In fact, attackers request continuously to access to the channel which results in undermining communication and limiting channel capacity. One of the countermeasures to such an attack is time-division multiplexing [48] allowing each node to transmit only in a specific time slot.

- Interrogation [49]:

To soften the problem of frame collisions introduced by the hidden node problem, several MAC protocols use the RTS/CTS handshake [50]. Attackers take advantages of this synchronization mechanism by repeatedly sending RTS packets leading to CTS responses from neighboring nodes. To counter this type of attack, nodes can use several mechanisms such as anti-replay protection and link layer authentication [51].

- Sybil Attack [52]:

As shown in figure 3 Sybil Attacks allow malicious nodes to have multiple identities by using the identities of the nodes targeted by the attack in order to participate in distributed algorithms such as election to take advantage of legitimate nodes to endorse the creation of several routes passing through the malicious node. This attack is located between the link and the network layers and it aims to degrade the integrity of data, the security level of and the use of resources. Among these attacks we can found Data Aggregation attacks aiming to falsify the aggregated message and Voting attacks affecting routing path and node selection. Several researches, such as [53] [54], sought to counter this attack using different mechanism such as public key cryptography and digital signatures.

- Sinkhole:

Sinkhole attack [55] belongs to DoS attacks in WSNs. As shown in figure 4, the attacker (malicious node) must appear to other nodes as being very attractive by presenting optimal routes in order to attract packets as much as possible to control most of

the data circulating in the network. Consequently, malicious node acts as a base station by attracting data packets and preventing them from continuing their path creating a kind of well or black hole in the network. The attacker, having a strategic routing location in the network, manipulates packets as desired, causing the suspension of the network routing service and the depletion of critical resources of nodes. Geo-routing protocols, using localized information and routing traffic through the physical location of nodes, are resistant to sinkhole attacks.

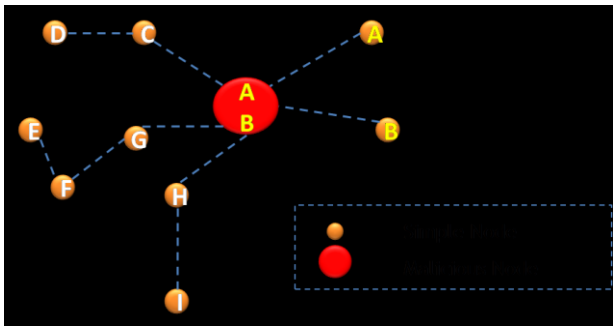

Figure 3: Sybil Attack

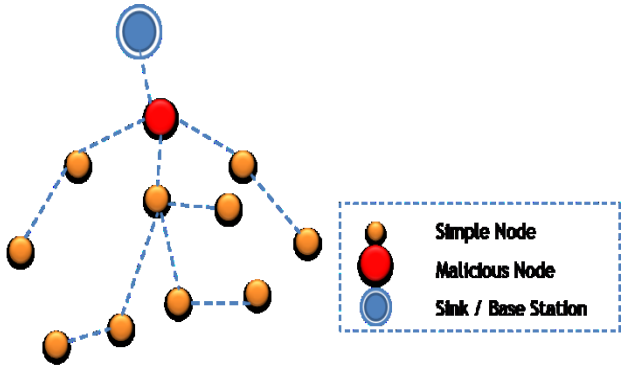

Figure 4: Sinkhole attack

- Hello Flood [56]:

The presence of laptop-class attackers and the limited transmission range of sensors led to the appearance of the Hello flood attacks. This attack takes advantages of the powerful signal of the attacking device to broadcast the information of an optimal route to all the nodes which will update their local tables. When a targeted node wants to communicate, it will not be able to use this route because the attacker, which is the imaginary neighbor, is out of range which results in the waste of energy from the sensors which leads to a malfunction of the network. Security mechanisms such as cryptography and source authentication, used to verify the bidirectionality of a path before taking action received over it, are used to counter this type of attacks.

- Node Capture:

In most applications, sensor nodes are highly vulnerable to physical attacks as they are often deployed in open areas easily accessible to attackers which raise the possibility of node capture to be used in tampering attacks. Researches such as [57] show that even a single node capture led to take over the entire network by attackers which makes the resilience against node capture attacks one of the most challenging issues in WSNs [58].

- Selective Forwarding:

Routing protocols assume that nodes will faithfully relay the packets that pass through them. We talk about Selective Forwarding attack when attacker may create malicious nodes and can violate this rule by removing all or some of these incoming packets randomly (neglectful node) or by giving high priority to its own messages (greedy node). Multipath routing, braided paths and random selection of paths to destination are a possible defense against this type of attack [59] [60].

- Black Hole Attack:

This attack can be considered as a form of selective forwarding attack dropping all incoming packets, it consists of inserting a new node or compromising a network node which falsifies the routing information to broadcast itself as the shortest path to oblige a maximum of neighbors to modify their routing tables in order to force the data to pass through it. This information will be destroyed which makes the malicious node as a well or black hole in the network. When attacker is placed on a strategic routing location in the network such as sinks or base stations the attack cause a network partition, packets loss, resource exhaustion and even the suspension of the routing services of the entire network. Black hole attack often targets hierarchical architectures and more specifically aggregator nodes. Multiple paths routing presents a defense against black hole attack [61] [62].

- Wormhole Attacks [63]:

Also known as tunneling, it is one of the most severe attacks. As shown in Figure 5, it requires at least two malicious nodes linked by a powerful radio link or by a wire link. In a wormhole attack, information received by a malicious node in one side of the network are encapsulated and relayed to be reintroduced by another malicious node on the other side of the network, revealing that the message originates from a close node. Encapsulation can be done in two ways: "Multi-hop encapsulation" aiming to hide intermediate nodes located between the two attackers to make the paths through the malicious node appear shorter which facilitates the creation of sinkholes with protocols using the number of hops as main metric of paths selection and "direct communication" in which paths going through the attackers are faster because they are composed of a single hop and can be used against protocols using the first discovered path and those based on paths latency. This type of attacks can considerably disrupt a location system by introducing erroneous reference points. It can be further divided into three classes: Half Open Wormhole, Closed Wormhole, and Open Wormhole. Several mechanisms for detecting and defending against wormhole attacks are presented such as WRHT [64].

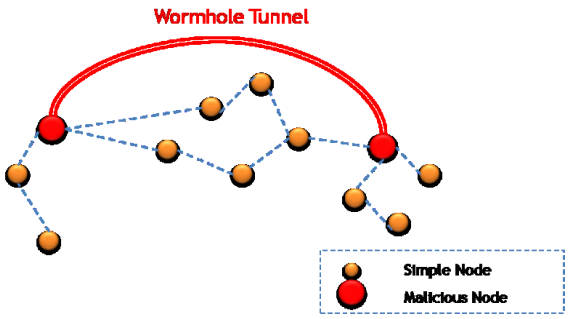

Figure 5: Wormhole attack

- Spoofed, Altered, or Replayed Routing Information [65]:

routing information in transit are targeted by several attacks, they can be spoofed, altered, or replayed. Malicious nodes can attract or repel the network traffic, inject false and misleading packets, overflow routing tables and create routing loops which result in disrupting the network traffic, partitioning the communication system and even destruction on the entire network. Several researches, such as [66], aim to counter these attacks using counters, timestamps, encryption and various authentication techniques.

- Misdirection [67]:

This active attack consists in misdirecting the data packets. In fact, instead of sending the packets in a correct direction, malicious nodes redirect them in a wrong direction through which the right destination is unreachable. Targeted node, flooded without any useful information, suffers from a waste of resources. Some security mechanisms [68] such as smart sleep [69] avoids this attack.

- Homing [70]:

This attack aims to locate critical nodes in the network providing essential services such as cluster heads and key managers by monitoring and analyzing the network traffic and nodes activities in order to eavesdrop their activities, take control of the network and extract sensitive data. To prevent homing attacks, protocols designers use different types of cryptographic schemes, algorithms and hide management messages [71] [72].

- Flooding [73]:

This attack aims to provoke a denial of service in order to decreases network lifetime. Indeed, one or several malicious nodes propagate many connection requests and carry out a regular massive sending to a strong emission power until exhausting the resources required the connection or reaching a maximum limit in order to saturate the network and prevent legitimate nodes from establishing communications which exhaust the resources (memory and energy) and reduce availability. One proposed solution to this attack is to demonstrate the commitment to this connection or to put a limit on the number of connections from a particular node [74] [75].

- De-synchronization Attacks [76]:

It is a part of the resource depletion attacks. The attacker causes missed frames by distorting, changing or increasing the sequence number of exchanged packets between end points. By receiving the modified packets, the destination deduces that the packets have been lost and requests the forwarding of these packets to the senders which disrupts the synchronization of communications and led to a considerable waste of energy of legitimate sensors by attempting to recover from errors which never really existed. Packets authentication is one of the main solutions to counter this attack [77] [78].

- Overwhelm attack [79]:

It is a part of QoS attacks. It consumes network bandwidth causing resource depletion by forwarding large amounts of data packets due to an exaggerated stimulation of sensors. A good adjustment of sensors and stimulation parameters, rate-limiting and efficient data-aggregation algorithms help to counter this attack [80].

- Path-based DOS attack [81]:

In this attack malicious nodes inject spurious or replayed packets in the network which waste energy resources and bandwidth on the path to the base station. Hence, legitimate nodes are prevented from sending packets to the base station. Authentication techniques and anti-replay protection counter this attack [82].

- Deluge (reprogram) attack [83]:

This attack uses one or more compromised nodes that the attacker reprograms them and then reinsert them on the network as malicious nodes working in his service. Deluge attack aims to disrupt the network and the application by causing an abnormal behavior of nodes. Indeed, these nodes run malicious codes in order to steal secret or sensitive information, attempt to disrupt the normal operation of the entire system and take control of large portions of a network. Several researches such as [84], introduce various techniques to counter this type of attacks.

Table 1 classifies the previously detailed routing attacks on WSNs according to our taxonomy proposed in the previous section.

4.2. *Simulation results*

4.2.1. Network model

To show the effect of these attacks on WSNs, we used the NS3 simulator to simulate the effect of Jamming and Hello Flood attacks on a WSN using LEACH protocol [85].

As indicated in Table2, the adopted network model consists of 100 nodes randomly deployed in 100m * 100m area with unlimited power sink centered in the field as shown in Figure 6.

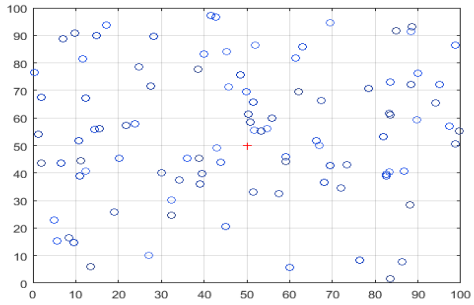

Figure 7: Nodes distribution

4.2.2. Results and discussion

In this section, the following metrics are used to evaluate the effect of Jamming and Hello Flood attacks:

- Network lifetime (Alive nodes Versus Rounds + Dead nodes Versus Rounds)

- Stability /instability periods

- Remaining energy Versus Rounds

We start with the evaluation of the network lifetime.

Table1: Comparison table of routing attacks in WSNs

Types / Attacks	Based On Protocol Stack					Based on the capability of the attacker				Based on the attack impact						Based on the attack target				Passive /active	
	PL	DLL	NL	TL	AL	LC		DC		IRP	ITC	M	F	RP	RD	U	H	S	I	P	A
						O	I	M	L												
Jamming	*	*	*			*	*	*	*	*					*		*				*
Tampering or destruction	*						*	*		*	*						*	*	*		*
Continuous Channel Access (Exhaustion)		*				*	*	*	*						*		*				*
Collision		*				*	*	*	*	*			*		*		*				*
Unfairness		*				*	*	*	*	*			*		*		*				*
Interrogation		*					*	*	*	*					*		*				*
Sybil Attack		*	*				*	*		*	*	*	*		*		*		*		*
Sinkhole			*				*	*		*	*	*	*	*	*		*		*	*	*
Hello Flood			*			*			*	*	*		*		*		*		*		*
Node Capture			*				*	*		*	*	*	*	*	*		*	*	*	*	*
Selective Forwarding			*				*	*		*	*	*	*		*		*		*		*
Black Hole Attack			*			*	*	*	*	*	*				*		*		*	*	
Wormhole Attacks			*				*		*	*	*	*			*		*		*		*
Spoofed, Altered, or Replayed Routing Information			*				*	*	*	*	*	*	*	*	*		*		*	*	*
Misdirection			*				*	*	*	*	*				*		*		*		*
Homing			*			*			*		*								*	*	
Flooding				*			*	*	*	*			*		*		*				*
De-synchronization Attacks				*			*	*	*	*		*			*		*		*		*
Overwhelm attack					*	*		*					*		*		*		*		*
Path-based DOS attack					*		*	*	*			*	*	*	*		*		*		*
Deluge (reprogram) attack					*		*	*		*	*	*	*	*	*		*	*	*		*

PL: Physical Layer
DLL: Data Link Layer
NL: Network Layer
TL: Transport Layer
AL: Application Layer
LC: Location Capability
O: Outsider
I: Insider
DC: Device Capability
M: Mote Class
L: Laptop Class
IRP: Interruption
ITC: Interception
M: Modification
F: Fabrication
RP: Reloading Packets
RD: Resources Depletion
U: Users
H: Hardware
S: Software
I: Information
P: Passive
A: Active

Table 2: Network parameters

Parameters	Values
Network size	100m * 100m
Number of nodes	100
Sink location	50,50
Packet size	4000 bits
Initial energy	0.5 J
Energy Dissipation (Efs)	10 pJ/bit/m²
Energy for transmission (ETx)	50 nJ
Energy for reception (ERx)	50 nJ
Data Aggregation	5 nJ/bit/report
Number of rounds	2000

- Network lifetime

The network lifetime is one of the main metrics to be considered to evaluate the efficiency of the network. It is the period between the beginning of the network and the death of last node. The two complementary Figures 8.a) and 8.b) respectively show the evolution of the number of alive and dead nodes in the network using LEACH protocol with and without the presence of attacks.

As shown in Figure 8, the network lifetime using LEACH protocol without undergoing attacks is about 1560 rounds, while it does not exceed 1080 rounds in the presence of Hello Flood attack and 820 rounds with Jamming attack. Using a powerful signal, Hello flood attack broadcast the information of an optimal imaginary route according to which the sensors update their local

tables. This technique led to a waste of energy and to a malfunction of the network. As explained earlier in this survey, deceptive Jamming attack, used in this simulation, consist in sending a constant data stream in the network which leads to overloading the antennas of the sensors and therefore to a great loss of energy and the disappearance of the network in a short time.

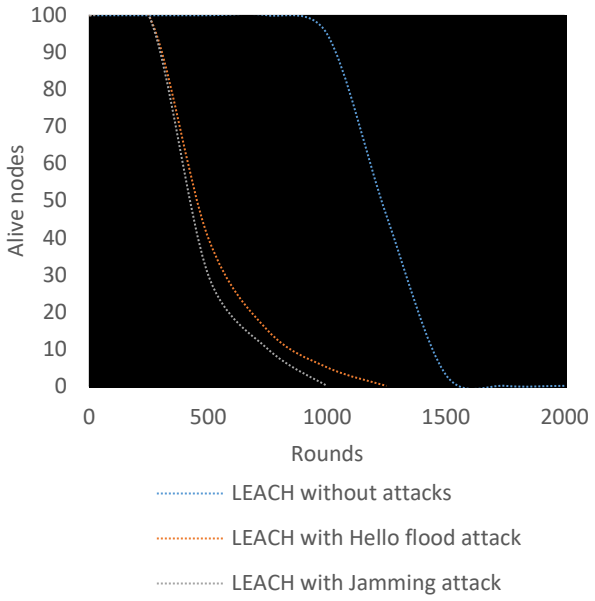

Figure 8-a: Alive nodes VS. rounds

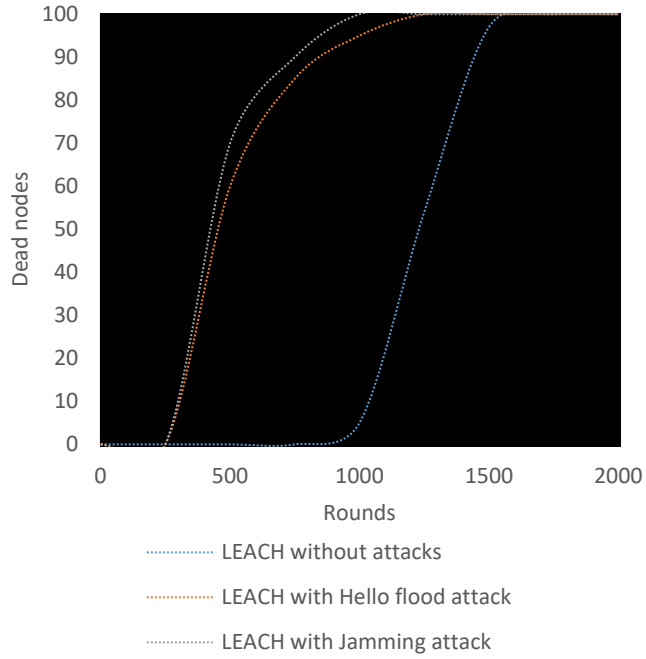

Figure 8-b: Dead nodes VS. rounds

Figure 8: Network lifetime

- Stability / instability period

A stability period triggers with the beginning of the network until the death of the first node which declares the beginning of an instability period. This instability period extends until the death of all nodes in the network. Figure 9 shows the stability and instability periods of the network using LEACH protocol with and without the presence of attacks.

As shown in Figure 9, the stability period almost reached 790rounds without attacks, but it does not exceed 320 rounds in the presence of Hello flood attack and 255 rounds with Jamming attack. In the same way, the instability period is about 773 rounds in the absence of attacks but does not surpass 760 rounds with Hello flood attack and 565 rounds in the presence of Jamming attack. This is obviously explained by the effect of the attacks on the consumption of energy.

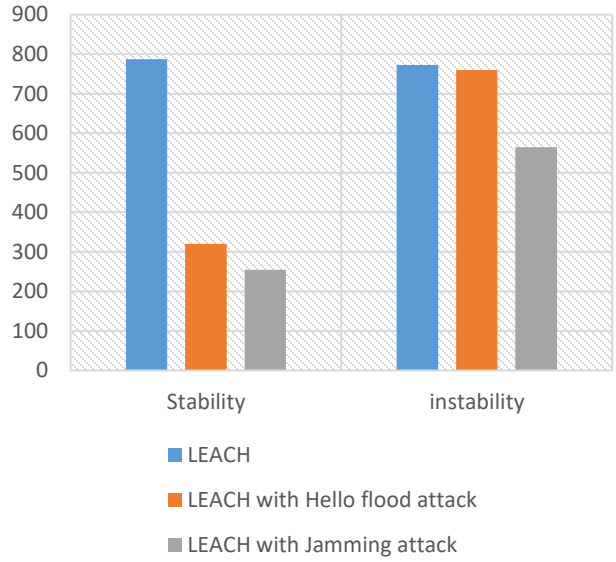

Figure 9: Stability and instability periods

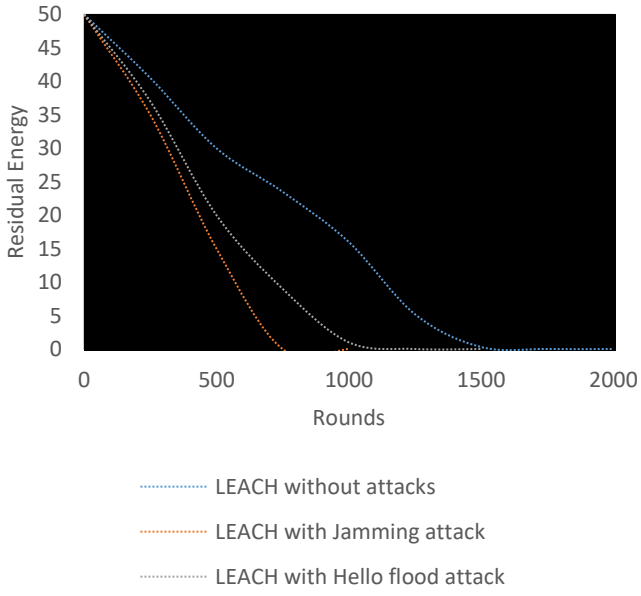

Figure 10: Residual Energy VS. Time

- Remaining energy

The residual energy, shown in Figure 10, results from the evolution of the number of nodes in the network. The curves show

the acute effect of the attacks on the residual energy of the network where half of the energy is consumed before reaching 500 rounds in the presence of attacks. The evolution of energy in this way leads to the formation of several isolated areas and subsequently affects the efficiency of the network.

In the following section, we present the main security mechanisms used to counter these attacks.

5. Basic security mechanisms in WSNs

In the absence of strong security architecture, WSNs are targets of several attacks that we presented previously in this paper. Most of these attacks take advantage of cryptographic system failures to derive the initial data (clear) or to find the used keys. We are talking here about cryptanalysis. In this section, we talk about cryptography and the cryptographic systems used to secure the WSNs [86] [87].

Indeed, the cryptanalysis targets the encryption keys which are based on cryptographic systems. These systems, that can be either symmetric, asymmetric or hybrid, take care of the management and distribution of the encryption keys [88] [89]. In the following, we detail each of these classes.

5.1. *Symmetric Cryptography in WSNs*

Symmetric cryptography, shown in Figure 11, is the oldest form of encryption where the same key is used between two communicating nodes to encrypt and decrypt the data using a symmetric encryption algorithm. In modern security techniques, even symmetric encryption algorithms can be public. The major disadvantage of this solution is that the pre-loaded key in the nodes could lead to compromise the entire network through compromised nodes. One of the proposed solutions to overcome this limit is to establish symmetric encryption schemes based on pair-wise keys rather than a single global key [90] [91].

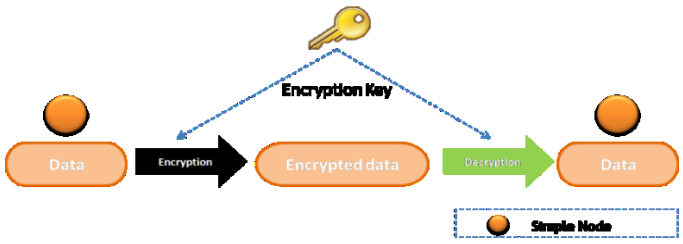

Figure 11: Symmetric cryptography

5.2. *Asymmetric Cryptography in WSNs*

Contrary to symmetric cryptography, asymmetric cryptography, also known as public-key cryptography, too heavy used in WSNs, uses a pair of keys instead of one (public and private). Asymmetric keys are generated in pairs. The message encrypted by the public key will be decrypted by the private key. Indeed, the public key of a node B, published between two communicating nodes is used by the node A to encrypt a message that will be decrypted by the node B through its secret private key as shown in Figure 12 and vice versa. This encryption mechanism allows not only the encryption of information but also the guarantee the authentication of the nodes by using the signatures and digital certificates. Slowness and resources consumption are the major drawbacks of this encryption mechanism [92].

Figure 12: Asymmetric cryptography

5.3. *Hybrid Cryptography in WSNs*

Hybrid cryptography is a cryptographic system that combines and benefits from the two cryptographic systems: asymmetric and symmetric. Generally, asymmetric encryption, greedy in time and resources, is used only to exchange a secret key in order to use symmetric encryption afterwards.

5.4. *Elliptic curve cryptography in WSNs*

Elliptic Curve Cryptography (ECC) is becoming increasingly popular as a security solution for WSNs. This technique is an approach of public-key cryptography, it is based on elliptic curve theory to create faster, smaller and more efficient encryption keys with quite less key size and very low computational overhead. In fact, the ECC generates keys through the properties of the elliptic curve equation and the discrete logarithm of an elliptic curve must be calculated for the decryption process which is much more difficult than factoring.

5.5. *Comparison of symmetric and asymmetric cryptographic systems*

Encryption algorithms can be evaluated in different parameters. Table 3, provided by National Institute of Standards and Technology NIST compares the encryption key size for RSA, ECC (asymmetric) and AES (symmetric) shows the development of key size compared to the security of an 80-bit symmetric key [93].

Table 3: Comparison of key length (bits) of the well-known symmetric and asymmetric techniques [NIST]

Symmetric (AES)	RSA	ECC
80	1024	160
112	2048(x 2)	224(x 1.4)
128	3072(x 3)	256 (x 1.6)
192	7680(x 7.5)	384(x 2.4)
256	15360(x 15)	521(x 3.2)

Researchers agree that symmetric methods are faster and require small keys e.g. a key size of 3072 bits with RSA, which is equivalent to 256 bits with ECC, offers the same level of security as a key of only 128 bits with AES. However, for a network of N nodes, N-1 symmetric keys must be stored in each node, which exceeds the memory capacity of sensors in networks that can contain thousands of nodes as well as the key distribution problem.

Figure 13, developed from experiments done using MATLAB R2015a [92] compares the energy consumed by RSA-1024 and ECC-160 for signatures generation and verification, and the energy cost of key exchanges excluding authentication and certificate verification. It shows that RSA is characterized by a very expensive signature operation and a small verification cost contrary to ECDSA signatures which are significantly cheaper than RSA. In the same way, key exchanging costs are significantly cheaper with ECDSA than with RSA.

As a result, the ECC has emerged as it offers keys that can be much smaller than those required by the RSA algorithm, and at the same time of size close to symmetrical solutions. These characteristics make this technique more suitable for WSNs and IoT applications but not optimal in its general form [94] [95].

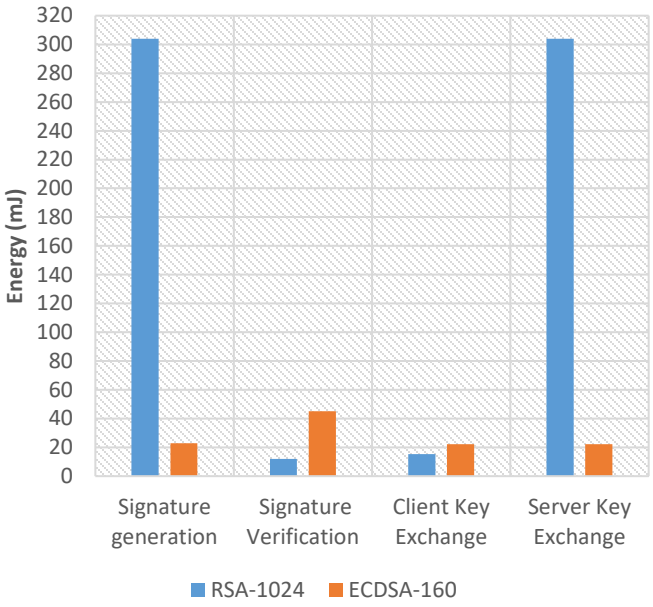

Figure 13: Energy cost of digital signature and key exchange using RSA-1024 and ECDSA-160

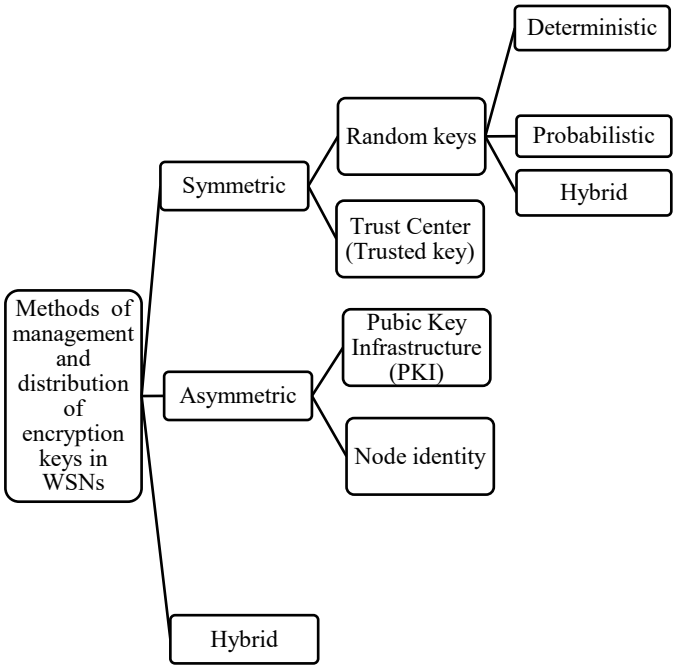

Figure 14: Methods of management and distribution of encryption keys in WSNs

5.6. *Management of encryption keys in WSNs*

Key management in WSNs is one of the most difficult aspects when configuring a security cryptographic system whether in a symmetric, asymmetric or hybrid-based method. This task includes the generation, distribution, verification and storage of encryption keys so that each node will be equipped with a set of secret keys or private/public pair of keys according to the adopted system in a secure, private and safe manner.

Several management classifications and key distribution have been proposed in the literature based on various technical and functional criteria [96]. We propose in this work a new classification based on the three previously proposed encryption methods (symmetric, asymmetric and hybrid) as shown in Figure 14. In the following we detail each of these key distribution methods.

5.7. *Management of encryption key in symmetric patterns*

The establishment of a common key between nodes in a WSNs to securely communicate in a symmetric cryptographic-based model is as follows: Before the nodes are deployed, the memory of each node is initially equipped with several keys in a Key Pre-distribution phase then it is the routing protocol that deals with the common key management between the nodes after the deployment in a key discovery process which makes it possible to constitute secure paths between nodes. The pre-distribution of these keys can be random or through an intermediary trust element of the network.

5.7.1. Random keys

The random pre-distribution of keys can be guaranteed by probabilistic, deterministic or hybrid methods. In the following we detail each of these methods

5.7.1.1. Deterministic methods

Deterministic methods require a large storage capacity because several encryption keys deterministically generated are stored in the memory of each node. They allow each node to establish a unique key known as “pair-wise key” with any other node of the network to establish a secure communication. Among the proposed mechanisms we quote the deterministic method proposed by Liu et al. [97] which is based on virtual spaces (logical grids) containing the identifiers of the nodes. Thus, many groups of sensor nodes are formed based on the positions of the nodes. The pre-distribution of two encryption keys is thus necessary: “in-group pre-distribution” making it possible to establish a unique shared key (pair-wise key) between two nodes of the same group and “cross-group pre-distribution” to establish a unique shared key between two different groups.

5.7.1.2. Probabilistic methods

In probabilistic methods, each node in the network is equipped with several encryption keys randomly chosen by the network administrator before being deployed. Common keys are thus installed in the memories of the nodes with a certain probability. In [98], Jones et al. propose a secure probabilistic architecture based on a probabilistic key distribution method. Indeed, each sensor is loaded with a set of “m” encryption keys, randomly selected from a set of “k” keys with a probability of matching "p" between nodes. After deployment, the BS splits the network into independent sectors and secret keys are distributed by the BS to ensure secure communication.

5.7.1.3. Hybrid methods

Hybrid pre-distribution methods combined and benefits from the two previous methods, depending on the application to increase connectivity between nodes while ensuring secure communication.

5.7.2. Trust Center

In this key pre-distribution model, a Trust Center e.g. the BS is used either to store a copy of pre-loaded keys or to derive encryption keys from a trusted key pre-loaded into the nodes. In a Zigbee topology managed by the protocol stack known as ZigBee [99] based on the IEEE 802.15.4 standard, the nodes can play three roles: coordinator, routers, and sensors. The coordinator, placed in a particular position in the network, plays the role of a Trust Center (TC) and distributes keys that can be Link Key (LK), Network Key (NK) or Master Key (MK) shared by one node respectively with another node, with the entire network and for the establishment of the key LK.

5.8. *Management of encryption key in asymmetric patterns*

Another way to establish a common key between two nodes or a group of nodes in a WSN to secure communications is to use schemes based on asymmetric systems as already explained. In the following we detail the most know methods.

5.8.1. Public Key Infrastructure

Public Key Infrastructure (PKI) based specifically on cryptography, are a set of protocols and services aiming to secure communication in a network through various techniques such as authentication, digital certificates, digital signatures etc. The Micro Public Key Infrastructure (micro-PKI) method proposed by Munivel et al. [100] for WSNs is based on two keys: a public key loaded in each node before the deployment used to identify with the BS and a private key used by the BS to decrypt the data sent by the nodes. The PKI in this method ensures identification between the nodes as well as with the BS.

5.8.2. Node identity

These methods seek to provide the same cryptographic services as a PKI based solely on the node identity information in the creation and establishment of cryptographic keys shared between each pair of nodes in the network. These methods are known in cryptography as the Identity-Based Non-Interactive Key Distribution Scheme (ID-NIKDS) [101]. Among these methods we quote the method proposed by Oliveira et al. [102] where each node of the network has a unique identifier and a private key. A unique secret key shared with another node of the network is derived by knowing only its identifier.

5.9. *Management of encryption key in hybrid patterns*

Hybrid cryptography is a system that combines the symmetric and asymmetric cryptography. It benefits from their advantages to ensure a high level of security in particular situations as mentioned previously in this work. The Transport Layer Security (TLS) [103] combines the two cryptographic systems. Indeed, as asymmetric cryptographic operations are very expensive, it is only used in the key distribution then a symmetric algorithm is used for the bulk encryption of the data.

In the following section, we summarize and discuss the results obtained in this survey.

6. Analysis and Findings

The specific characteristics of WSNs, usually deployed in hostile environments make these networks targeted by various types of attacks which can target all components of the network such as nodes, routes, packets etc. Simulation results show that the network lifetime can decrease by more than 45% as in the presence of Jamming attack. These conditions lead us to discuss the existing security techniques which, despite their proven effectiveness with other types of networks, cannot be directly adapted to the limited resources of sensors and a new security mechanism taking advantage of existing solutions must be proposed.

7. Conclusion and future work

As an involving field, WSNs usually used in unattended environments and characterized by limited resources become vulnerable to several types of attacks targeting all network components such as nodes, packets and routing protocols etc. In this paper, we aim to facilitate the design and implementation of reliable and secure routing protocols for researchers. So, we summarize the security requirements for WSNs then we propose a new taxonomy distinguishing four possible categories of attacks namely: attacks based on the protocol stack, based on the capability of the attacker, based on the attack impacts and based on the attack target. Then, we classify and analyze the most known attacks based on the proposed model and using the NS3 simulator. Thereafter, we present and discuss the basic security methods and protocols of management and distribution of encryption keys in WSNs.

Security Mechanisms in WSNs, used to counter these attacks in order to keep the network running smoothly will be the objective of our future work aiming to propose a new security method which will be adapted to the specific properties of WSNs and able to counter the majority of these attacks.

References

[1] YADAV, Devendra, SINGAM, Jayanthu, DAS, Santos, et al. A Critical Review on Slope Monitoring Systems with a Vision of Unifying WSN and IoT. IET Wireless Sensor Systems, 2019.

[2] PRABHU, Boselin, BALAKUMAR, N., et ANTONY, A. Johnson. Wireless Sensor Network Based Smart Environment Applications. 2017.

[3] SHAHZAD, Furrakh, PASHA, Maruf, et AHMAD, Arslan. A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. arXiv preprint arXiv:1702.07136, 2017.

[4] SENGAR, P. et BHARDWAJ, N. A Survey on Security and Various Attacks in Wireless Sensor Network. International Journal of Computer Sciences and Engineering, 2017, vol. 5, no 4, p. 78-84.

[5] MITTAL, Vikas, GUPTA, Sunil, et CHOUDHURY, Tanupriya. Comparative Analysis of Authentication and Access Control Protocols Against Malicious Attacks in Wireless Sensor Networks. In : Smart Computing and Informatics. Springer, Singapore, 2018. p. 255-262.

[6] BANA, Suman et BAGHLA, Silki. Wireless sensor network. International Journal of Engineering Science, 2016, vol. 1706.

[7] Kardi, A., Zagrouba, R., & Alqhtani, M. (2018, May). Hierarchical Routing Techniques in Wireless Sensor Networks. In International Symposium on

Web and Wireless Geographical Information Systems (pp. 77-84). Springer, Cham.
[8] TOMIĆ, Ivana et MCCANN, Julie A. A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols. IEEE Internet of Things Journal, 2017, vol. 4, no 6, p. 1910-1923.
[9] CUI, Jie, SHAO, Lili, ZHONG, Hong, et al. Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks. Peer-to-Peer Networking and Applications, 2017, p. 1-16.
[10] ORACEVIC, Alma, DILEK, Selma, et OZDEMIR, Suat. Security in internet of things: A survey. In : Networks, Computers and Communications (ISNCC), 2017 International Symposium on. IEEE, 2017. p. 1-6.
[11] DAS, Ashok Kumar. A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor. International Journal of Communication Systems, 2017, vol. 30, no 1.
[12] MENDEZ, Diego M., PAPAPANAGIOTOU, Ioannis, et YANG, Baijian. Internet of things: Survey on security and privacy. arXiv preprint arXiv:1707.01879, 2017.
[13] PRITCHARD, Sean W., HANCKE, Gerhard P., et ABU-MAHFOUZ, Adnan M. Security in Software-Defined Wireless Sensor Networks: Threats, Challenges and Potential Solutions. In : IEEE Int. Conf. of Ind. Informat., Emden, Germany. 2017.
[14] SHAHZAD, Furrakh, PASHA, Maruf, et AHMAD, Arslan. A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. arXiv preprint arXiv:1702.07136, 2017.
[15] ZHU, Liehuang, ZHANG, Zijian, et XU, Chang. Secure data aggregation in wireless sensor networks. In : Secure and Privacy-Preserving Data Communication in Internet of Things. Springer, Singapore, 2017. p. 3-31.
[16] MATHEW, Prabha Susy, PILLAI, Anitha S., et PALADE, Vasile. Applications of IoT in Healthcare. In : Cognitive Computing for Big Data Systems Over IoT. Springer, Cham, 2018. p. 263-288.
[17] TOMIĆ, Ivana et MCCANN, Julie A. A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols. IEEE Internet of Things Journal, 2017, vol. 4, no 6, p. 1910-1923.
[18] ZHANG, Anran et BAI, Fengshan. An energy efficient and dynamic time synchronization protocol for wireless sensor networks. In : Seventh International Conference on Electronics and Information Engineering. International Society for Optics and Photonics, 2017. p. 103221X.
[19] LI, Peng, YU, Xiaotian, XU, He, et al. Research on secure localization model based on trust valuation in wireless sensor networks. Security and Communication Networks, 2017, vol. 2017.
[20] LI, Xiong, NIU, Jianwei, KUMARI, Saru, et al. A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. Journal of Network and Computer Applications, 2018, vol. 103, p. 194-204.
[21] ALIBERTI, Giulio, DI PIETRO, Roberto, et GUARINO, Stefano. Epidemic data survivability in Unattended Wireless Sensor Networks: New models and results. Journal of Network and Computer Applications, 2017, vol. 99, p. 146-165.
[22] ZHANG, Junqing, DUONG, Trung Q., WOODS, Roger, et al.Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview. Entropy, 2017, vol. 19, no 8, p. 420.
[23] DENER, Murat et BAY, Omer Faruk. Practical Implementation of an Adaptive Detection-Defense Unit against Link Layer DoS Attacks for Wireless Sensor Networks. Security and Communication Networks, 2017, vol. 2017.
[24] SAINI, Rakesh Kumar, RITIKA, Ritika, et VIJAY, Sandip. Data Flow in Wireless Sensor Network Protocol Stack by using Bellman-Ford Routing Algorithm. Bulletin of Electrical Engineering and Informatics, 2017, vol. 6, no 1, p. 81-87.
[25] KİRAZ, Ayhan et ÇAKIROĞLU, Murat. ALORT: a transport layer protocol using adaptive loss recovery method for WSN. Sādhanā, 2017, vol. 42, no 7, p. 1091-1102.
[26] LI, Xiaomin, LI, Di, WAN, Jiafu, et al. A review of industrial wireless networks in the context of industry 4.0. Wireless networks, 2017, vol. 23, no 1, p. 23-41.
[27] CHOI, Jaewoo, BANG, Jihyun, KIM, LeeHyung, et al. Location-based key management strong against insider threats in wireless sensor networks. IEEE Systems Journal, 2017, vol. 11, no 2, p. 494-502.
[28] TYAGI, Akshat, KUSHWAH, Juhi, et BHALLA, Monica. Threats to security of Wireless Sensor Networks. In : Cloud Computing, Data Science & Engineering-Confluence, 2017 7th International Conference on. IEEE, 2017. p. 402-405.
[29] GRGIC, Kresimir, MENDELSKI, Vedran, et ZAGAR, Drago. Security framework for visual sensors and smart camera networks. In : Telecommunications (ConTEL), 2017 14th International Conference on. IEEE, 2017. p. 131-138.
[30] JAITLY, Sunakshi, MALHOTRA, Harshit, et BHUSHAN, Bharat. Security vulnerabilities and countermeasures against jamming attacks in Wireless Sensor Networks: A survey. In : Computer, Communications and Electronics (Comptelix), 2017 International Conference on. IEEE, 2017. p. 559-564.
[31] SHAHZAD, Furrakh, PASHA, Maruf, et AHMAD, Arslan. A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. arXiv preprint arXiv:1702.07136, 2017.
[32] BHUSHAN, Bharat et SAHOO, Gadadhar. Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks. Wireless Personal Communications, 2017, p. 1-41.
[33] SENNIAPPAN, Vijayalakshmi et SUBRAMANIAN, Jayashree. Threshold-based Energy Efficient Clustering Protocol for Corrosion Risk Monitoring of Reinforced Concrete. International Journal of Computer Applications, 2017, vol. 157, no 6.
[34] RAMACHANDRAN, Shyamala et SHANMUGAM, Valli. Impact of DoS Attack in Software Defined Network for Virtual Network. Wireless Personal Communications, 2017, vol. 94, no 4, p. 2189-2202.
[35] DESNITSKY, Vasily et KOTENKO, Igor. Modeling and Analysis of IoT Energy Resource Exhaustion Attacks. In : International Symposium on Intelligent and Distributed Computing. Springer, Cham, 2017. p. 263-270.
[36] SHAHZAD, Furrakh, PASHA, Maruf, et AHMAD, Arslan. A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. arXiv preprint arXiv:1702.07136, 2017.
[37] VADLAMANI, Satish, EKSIOGLU, Burak, MEDAL, Hugh, et al. Jamming attacks on wireless networks: A taxonomic survey. International Journal of Production Economics, 2016, vol. 172, p. 76-94.
[38] SHABANA, Kalsoom, FIDA, Nigar, KHAN, Fazlullah, et al. Security issues and attacks in Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), 2016, vol. 5, no 7, p. pp: 81-87.
[39] ZHU, Jia, ZOU, Yulong, et ZHENG, Baoyu. Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks. IEEE Access, 2017..
[40] BHAVATHANKAR, Prasenjit, SARKAR, Subhadeep, et MISRA, Sudip. Optimal decision rule-based ex-ante frequency hopping for jamming avoidance in wireless sensor networks. Computer Networks, 2017.
[41] DINKER, Aarti Gautam et SHARMA, Vidushi. Attacks and challenges in wireless sensor networks. In : Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on. IEEE, 2016. p. 3069-3074.
[42] DINKER, Aarti Gautam et SHARMA, Vidushi. Attacks and challenges in wireless sensor networks. In : Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on. IEEE, 2016. p. 3069-3074.
[43] DENER, Murat et BAY, Omer Faruk. Practical Implementation of an Adaptive Detection-Defense Unit against Link Layer DoS Attacks for Wireless Sensor Networks. Security and Communication Networks, 2017, vol. 2017.
[44] MISHRA, Alekha Kumar. Security Threats in Wireless Sensor Networks. Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures, 2016, p. 307.
[45] JAN, Mian Ahmad et KHAN, Muhammad. Denial of Service Attacks and Their Countermeasures in WSN. IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), 2013, vol. 3.
[46] REN, Ju, ZHANG, Yaoxue, ZHANG, Kuan, et al. Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks. IEEE Transactions on Wireless Communications, 2016, vol. 15, no 5, p. 3718-3731.
[47] MOHAMMADI, Shahriar et JADIDOLESLAMY, Hossein. A comparison of link layer attacks on wireless sensor networks. arXiv preprint arXiv:1103.5589, 2011.
[48] NEWAZ, SH Shah, CUEVAS, Ángel, LEE, Gyu Myoung, et al. Improving energy saving in time-division multiplexing passive optical networks. IEEE Internet Computing, 2013, vol. 17, no 1, p. 23-31.
[49] SINGLA, Aashima et SACHDEVA, Ratika. Review on security issues and attacks in wireless sensor networks. International Journal of Advanced Research in Computer Science and Software Engineering, 2013, vol. 3, no 4.
[50] KAUR, Ramandeep et SHARMA, Reecha. An Analysis of RTS/CTS Mechanism for Data Transfer In Wireless Network: A Review. 2016.
[51] GHEORGHE, Laura, RUGHINIS, Razvan, DEACONESCU, Razvan, et al. Authentication and anti-replay security protocol for wireless sensor networks. In : Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on. IEEE, 2010. p. 7-13.
[52] LI, Xun, HAN, Guangjie, QIAN, Aihua, et al. Detecting Sybil attack based on state information in Underwater Wireless Sensor Networks. In : Software, Telecommunications and Computer Networks (SoftCOM), 2013 21st International Conference on. IEEE, 2013. p. 1-5.

[53] JAN, Mian Ahmad, NANDA, Priyadarsi, HE, Xiangjian, et al. A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network. In : Trustcom/BigDataSE/ISPA, 2015 IEEE. IEEE, 2015. p. 318-325.

[54] JAN, Mian Ahmad, NANDA, Priyadarsi, HE, Xiangjian, et al. A sybil attack detection scheme for a forest wildfire monitoring application. Future Generation Computer Systems, 2016.

[55] SHAFIEI, Hosein, KHONSARI, Ahmad, DERAKHSHI, H., et al. Detection and mitigation of sinkhole attacks in wireless sensor networks. Journal of Computer and System Sciences, 2014, vol. 80, no 3, p. 644-653.

[56] SINGH, Virendra Pal, UKEY, Aishwarya S. Anand, et JAIN, Sweta. Signal strength based hello flood attack detection and prevention in wireless sensor networks. International Journal of Computer Applications, 2013, vol. 62, no 15.

[57] LIN, Chi et WU, Guowei. Enhancing the attacking efficiency of the node capture attack in WSN: a matrix approach. The Journal of Supercomputing, 2013, vol. 66, no 2, p. 989-1007.

[58] TAHIR, Ruhma et MCDONALD-MAIER, Klaus. Improving resilience against node capture attacks in wireless sensor networks using icmetrics. In : Emerging Security Technologies (EST), 2012 Third International Conference on. IEEE, 2012. p. 127-130.

[59] REN, Ju, ZHANG, Yaoxue, ZHANG, Kuan, et al. Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks. IEEE Transactions on Wireless Communications, 2016, vol. 15, no 5, p. 3718-3731.

[60] SHAHZAD, Furrakh, PASHA, Maruf, et AHMAD, Arslan. A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. arXiv preprint arXiv:1702.07136, 2017.

[61] BASKAR, Radhika, RAJA, PC Kishore, JOSEPH, Christeena, et al. Sinkhole Attack in Wireless Sensor Networks-Performance Analysis and Detection Methods. Indian Journal of Science and Technology, 2017, vol. 10, no 12.

[62] ALJUMAH, Abdullah et AHANGER, Tariq Ahamed. Futuristic Method to Detect and Prevent Blackhole Attack in Wireless Sensor Networks. International Journal of Computer Science and Network Security (IJCSNS), 2017, vol. 17, no 2, p. 194.

[63] SHAHZAD, Furrakh, PASHA, Maruf, et AHMAD, Arslan. A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. arXiv preprint arXiv:1702.07136, 2017.

[64] SINGH, Rupinder, SINGH, Jatinder, et SINGH, Ravinder. WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks. Mobile Information Systems, 2016, vol. 2016.

[65] MULLA, Ms Raisa I. et PATIL, Rahul. Review of Attacks on Wireless Sensor Network and their Classification and Security. Imperial Journal of Interdisciplinary Research, 2016, vol. 2, no 7.

[66] DINKER, Aarti Gautam et SHARMA, Vidushi. Attacks and challenges in wireless sensor networks. In : Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on. IEEE, 2016. p. 3069-3074.

[67] YOUNIS ABDULLAH, Maan, HUA, Gui Wei, et ALSHARABI, Naif. Wireless sensor networks misdirection attacker challenges and solutions. In : Information and Automation, 2008. ICIA 2008. International Conference on. IEEE, 2008. p. 369-373.

[68] SAINI, Meenu, KUMAR, Rajan, et al. To Propose a Novel Technique for Detection and Isolation of Misdirection Attack in Wireless Sensor Network. Indian Journal of Science and Technology, 2016, vol. 9, no 28.

[69] ABDALZAHER, Mohamed S., SEDDIK, Karim, ELSABROUTY, Maha, et al. Game Theory Meets Wireless Sensor Networks Security Requirements and Threats Mitigation: A Survey. Sensors, 2016, vol. 16, no 7, p. 1003.

[70] KURBAH, Rangstone Paul et SHARMA, Bobby. Survey On Issues In Wireless Sensor Networks: Attacks and Countermeasures. International Journal of Computer Science and Information Security, 2016, vol. 14, no 4, p. 262.

[71] AGRAWAL, Dharma Prakash. Authentication, Encryption, and Secured Communication. In : Embedded Sensor Systems. Springer Singapore, 2017. p. 393-413.

[72] SARANYA, K., SATHYA, D., et KUMAR, P. Ganesh. A Survey On Intrusion Detection System In Wireless Sensor Networks. International Journal of Advance Research, Ideas and Innovations in Technology. 2017, vol. 3, no 1, p. 692-703

[73] MANOHAR, Ram Pradheep et BABURAJ, E. Detection of Stealthy Denial of Service (S-DoS) Attacks in Wireless Sensor Networks. International Journal of Computer Science and Information Security, 2016, vol. 14, no 3, p. 343.

[74] ACHARJYA, D. P. et AHMED, N. Syed Siraj. Recognizing Attacks in Wireless Sensor Network in View of Internet of Things. In : Internet of Things: Novel Advances and Envisioned Applications. Springer International Publishing, 2017. p. 149-172.

[75] MANSOURI, Djamel, MOKDAD, Lynda, BEN-OTHMAN, Jalel, et al. Dynamic and adaptive detection method for flooding in wireless sensor networks. International Journal of Communication Systems, 2017.

[76] SHAHID, Jahanzeb, SALEEM, Shahzad, et QURESHI, Muhammad Nauman. DOS Attacks on WSN and Their Classifications With Countermeasures-A Survey. NUST Journal of Engineering Sciences, 2016, vol. 9, no 2.

[77] CAPOSSELE, Angelo T., CERVO, Valerio, PETRIOLI, Chiara, et al. Counteracting Denial-of-Sleep Attacks in Wake-up-radio-based Sensing Systems. In : Sensing, Communication, and Networking (SECON), 2016 13th Annual IEEE International Conference on. IEEE, 2016. p. 1-9.

[78] GOPE, Prosanta, LEE, Jemin, et QUEK, Tony QS. Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks. IEEE Sensors Journal, 2016, vol. 17, no 2, p. 498-503.

[79] GARCIA-FONT, Victor, GARRIGUES, Carles, et RIFÀ-POUS, Helena. Attack Classification Schema for Smart City WSNs. Sensors, 2017, vol. 17, no 4, p. 771.

[80] DINKER, Aarti Gautam et SHARMA, Vidushi. Attacks and challenges in wireless sensor networks. In : Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on. IEEE, 2016. p. 3069-3074.

[81] DENG, Jing, HAN, Richard, et MISHRA, Shivakant. Defending against path-based DoS attacks in wireless sensor networks. In : Proceedings of the 3rd ACM workshop on Security of adhoc and sensor networks. ACM, 2005. p. 89-96.

[82] DHAKNE, A. R. et CHATUR, P. N. Detailed Survey on Attacks in Wireless Sensor Network. In : Proceedings of the International Conference on Data Engineering and Communication Technology. Springer Singapore, 2017. p. 319-331.

[83] SARANYA, K., SATHYA, D., et KUMAR, P. Ganesh. A Survey On Intrusion Detection System In Wireless Sensor Networks. In the proceeding of the 2nd International Conference on Engineering Technology, Science and Management Innovation (ICETSMI- 2017)- India, January 2017. P, 158-165

[84] SAINI, Meenu, KUMAR, Rajan, et al. To Propose a Novel Technique for Detection and Isolation of Misdirection Attack in Wireless Sensor Network. Indian Journal of Science and Technology, 2016, vol. 9, no 28.

[85] ZHENSHAN, Bao, BO, Xue, et WENBO, Zhang. HT-LEACH: An improved energy efficient algorithm based on LEACH. In : Mechatronic Sciences, Electric Engineering and Computer (MEC), Proceedings 2013 International Conference on. IEEE, 2013. p. 715-718.

[86] RADHAPPA, Harish, PAN, Lei, XI ZHENG, James, et al.Practical overview of security issues in wireless sensor network applications. International Journal of Computers and Applications, 2017, p. 1-12.

[87] HE, Daojing, CHAN, Sammy, et GUIZANI, Mohsen. Cyber Security Analysis and Protection of Wireless Sensor Networks for Smart Grid Monitoring. IEEE Wireless Communications, 2017, vol. 24, no 6, p. 98-103.

[88] SINGH, Pooja et CHAUHAN, R. K. A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN. International Journal of Electrical and Computer Engineering, 2017, vol. 7, no 4, p. 2232.

[89] ZHANG, Ping, WANG, Shaokai, GUO, Kehua, et al. A secure data collection scheme based on compressive sensing in wireless sensor networks. Adhoc Networks, 2018, vol. 70, p. 73-84.

[90] CHELLI, Kahina. Security issues in wireless sensor networks: attacks and countermeasures. In : Proceedings of the World Congress on Engineering. 2015. p. 1-3.

[91] LI, Juan. A Symmetric Cryptography Algorithm in Wireless Sensor Network Security. International Journal of Online Engineering (iJOE)

[92] CHELLI, Kahina. Security issues in wireless sensor networks: attacks and countermeasures. In : Proceedings of the World Congress on Engineering. 2015. p. 1-3.

[93] KARDI, Amine, ZAGROUBA, Rachid, et ALQAHTANI, Mohammed. Performance Evaluation of RSA and Elliptic Curve Cryptography in Wireless Sensor Networks. In : 2018 21st Saudi Computer Society National Computer Conference (NCC). IEEE, 2018. p. 1-6.

[94] LI, Xiong, NIU, Jianwei, BHUIYAN, Md ZakirulAlam, et al. A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things. IEEE Transactions on Industrial Informatics, 2018, vol. 14, no 8, p. 3599-3609.

[95] IQBAL, Ummer et SHAFI, Saima. A Provable and Secure Key Exchange Protocol Based on the Elliptical Curve Diffe–Hellman for WSN. In : Advances in Big Data and Cloud Computing. Springer, Singapore, 2019. p. 363-372.

[96] BOJANOVA, Irena, BLACK, Paul E., et YESHA, Yaacov. Cryptography classes in bugs framework (BF): Encryption bugs (ENC), verification bugs (VRF), and key management bugs (KMN). In : Software Technology Conference (STC), 2017 IEEE 28th Annual. IEEE, 2017. p. 1-8.

[97] LIU, Donggang, NING, Peng, et DU, Wenliang. Group-based key predistribution for wireless sensor networks. ACM Transactions on Sensor Networks (TOSN), 2008, vol. 4, no 2, p. 11.
[98] JONES, K., WADAA, Ashraf, OLARIU, Stephan, et al. Towards a new paradigm for securing wireless sensor networks. In : Proceedings of the 2003 workshop on New security paradigms. ACM, 2003. p. 115-121.
[99] http://www.zigbee.org/.
[100] MUNIVEL, E. et AJIT, G. M. Efficient public key infrastructure implementation in wireless sensor networks. In : Wireless Communication and Sensor Computing, 2010. ICWCSC 2010. International Conference on. IEEE, 2010. p. 1-6.
[101] MALEH, Yassine et EZZATI, Abdellah. An advanced Study on Cryptography Mechanisms for Wireless Sensor Networks. arXiv preprint arXiv:1609.05323, 2016.
[102] OLIVEIRA, Leonardo B., ARANHA, Diego F., GOUVÊA, Conrado PL, et al. TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. Computer Communications, 2011, vol. 34, no 3, p. 485-493.
[103] DIERKS, Tim. The transport layer security (TLS) protocol version 1.2. IETF RFC 5246, August 2008.