International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 1696-1706 www.ijaem.net ISSN: 2395-5252

Security Challenges And Security Protocols For Wireless Sensor Networks: A Review

Hala Mohammad Yaroub[1] ,
Assist. Prof. Dr Jolan Rokan Naif[2] ,
Dr. Shatha Mezher Hasan[3]
Iraqi Commission for Computer & Informatics/ Informatics Institute for Postgraduate Studies, Iraq

----
Date of Submission: 20-08-2022 Date of Acceptance: 31-08-2022

ABSTRACT:WSN is a network of small interconnected sensors with limited resources, these devices communicate with each other wirelessly to collect data about the environment in which they are located and according to the application for which they are located.

There are many challenges and difficulties that the WSN faces including security, power consumption, production costs, memory size, etc. There are great efforts and a lot of research to develop these networks despite the challenges they face. Due to resource constraints, security is one of the most important challenges for WSNs when it comparing with traditional wired networks. As wireless communications are more prone to security breaches, it is easy to change data, enter wrong data, or eavesdrop and spy on data transmitted over the network. Therefore, many security protocols have been found that are used with applications, and each application deals with the protocol that complies with its security requirements.

This paper presents an overview of Wireless Sensor Networks, the requirements of security, the attacks that WSNs generally encounter more than others, and the protocols that are commonly used more than others in Wireless Sensor Network Security.

Keywords: WSNs, Security protocol, Security requirements, security Challenges, WSN attacks.

I. INTRODUCTION

A wireless sensor network is an infrastructure-free, self-configured wireless network that is used to monitor various physical and environmental factors, Depending on the nature of use. Wireless Sensor Networks (WSNs) are made up of from a few to hundreds of thousands of sensor nodes scatter over a region (sensing field) and one sink node or more. The application environment data is transferred from node to node down to the sink node, and in other applications, the data is transferred once from the node to the sink node directly, where the data is analyzed and processed. The sinks act as interfaces between user data and the network, so the user can retrieve processed data from the sink node through queries. These sensor nodes connect with one another via radio signals, and each sensor node in a Wireless sensor network is naturally limited resource constrained such as processing speed, storage space, and communication bandwidth [1].

In wireless sensor networks, because the data transfer through the air, it might be easy for an opponent to snoop on the traffic. Also, sensor nodes tend not to be manipulated to achieve the stringent balancing limitations requirements and thus do not provide any defense against security assaults. In addition to these weaknesses, human assistance is never permitted to deal with intruders trying to compromise the network. So, security systems are primarily required to protect against security risks and secure the network [2].

When wireless networks are attacked, this can result in serious consequences, so it requires the secure transmission of the obtained data to the intended recipient. For security weaknesses, protocols are created based on information security concepts including integrity, confidentiality, authentication, non-repudiation, and availability [3]. Wireless sensor networks can be secured using security schemes, however, doing so is exceedingly challenging given their resource constraints. Some researchers are seeking improved development of WSN protocols, others are trying to get better node designs, and still, others are trying to address security concerns, including the major security threat to WSNs from insecure radio links with the potential for eavesdropping and information corruption [4].

II. WIRELESS SENSOR NETWORK ARCHITECTURE

The following are the basic components of a typical wireless sensor network[5]:

2.1. Sensor Field (Sensor Node)

Every sensor node is made up of four main components: The Sensing unit, the Processing unit, the Transceiver, and the Power unit, as shown in Figure(1). The Sensing Unit has subunits that are: Sensors and ADCs (Analog to Digital Converter). The Processing Unit also contains two units, the Processor and the Storage. Location Finding System unit, as the sensor node requires some knowledge from other nodes and the accurate routing path, so this component achieves this goal. A Mobilizer module will be required when sometimes a sensor node needs to go in different directions to know the assigned tasks and this component can figure out the specific task. A Power Generator will act as a backup power generator in the event of any failure in the power unit [6].

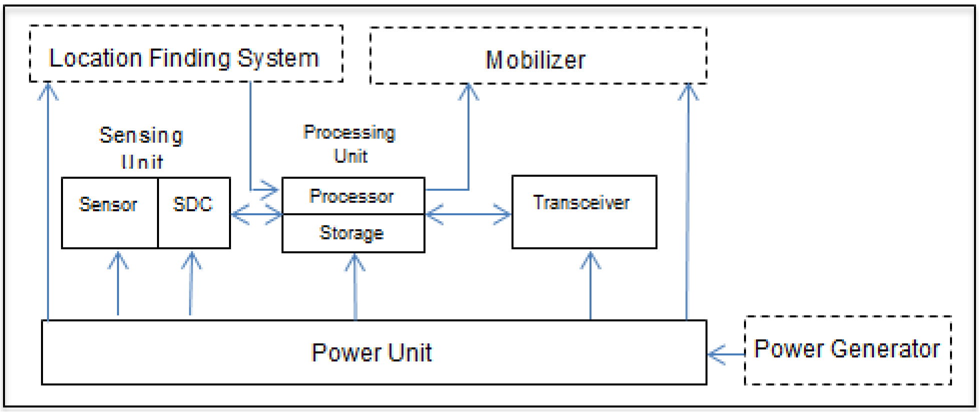


Figure (1): Component of the Sensor Node [7]

2.2. Gateway or Access point

A gateway enables contact between the host and the sensor field[5].

2.3. Network Manager

The network manager is responsible for organizing and scheduling the network configuration of the base stations as one or more valuable WSN components to many numbers of resources of distinct components for energy and communication computing[5].

III. WIRELESS SENSOR NETWORK CHALLENGES

The complication of big wireless sensor networks makes up considerable challenges to create protection and security strategies. Where the most important challenges faced by wireless sensor networks are security issues. Among the applications that need to provide security more than others are health care applications and military applications [5].

- ➢ Wireless Media:Wireless media is inherently less secure because of how simple eavesdropping is due to its broadcast nature. The wireless media makes it simple for an attacker to intercept valid packets and inject fake packets, and also any transmission can be instantly intercepted, altered, or replayed by an intrusion. The current methods must be updated to function effectively on wireless sensor networks.
- ➢ Ad-Hoc Deployment: The sensor networks lack a steadily specified structure due to their ad hoc construction. Nodes can be deployed Use the Airdrop so prior to deployment nothing is known about the topology. Due to the network must support nodes that might fail or be configuring themselves when it is replaced, security measures must be able to function in this dynamic environment.
- ➢ The Environment of Hostility:The hostile environment in which sensor nodes function is another potential risk element. The very hostile environment presents a big challenge to the security researchers.
- ➢ Massive Scale: The suggested size of the wireless sensor networks is a significant problem for security schemes. The easy networking of tens to thousands of nodes has proven to be a big challenge.

IV. SECURITY REQUIREMENTS

To preserve information and resources from attacks and misconduct, WSN security services must be ensured. WSN security requirements include confidentiality, availability, authentication, integrity, authorization, data freshness, non-repudiation, robustness, time synchronization, secure localization, and self-organization [4].

4.1. Confidentiality

The secrecy of data sent between nodes must be kept. Therefore, the data must be encrypted to prevent the attackers from understanding it. In several dynamic WSN systems where sensor nodes continue failing and quit the network then new nodes join to network, the forward secrecy and backward secrecy should be maintained. Forward Secrecy indicates that nodes that leave the WSN cannot read future data that will be transmitted on the WSN after leaving, and Backward Secrecy means that new nodes cannot read past data sent before joining the network [8].

4.2. Availability

Ensures that the required data can be obtained on time. Therefore, to ensure that data is continuously available, the sensor nodes must be available. If a sensor node is seized by an opponent or one of the nodes fails then the available data will be lost. So, the continuity of the operation of network applications must be preserved even in the event of availability loss [9].

4.3.Authentication

The Authentication of data prohibits illicit nodes from sharing in the network,and the original nodes are allowed to detect unauthorized nodes' messages[10].

4.4. Integrity

Ensure that the data transmitted over the network cannot be modified by attackers, and if this happens, the network should be able to detect those modifications [8].

4.5. Authorization

Guarantee that just the authorized devices are allowed participate in supplying WSN with data[11].

4.6. Data Freshness

Data Freshness service indicates the novelty of data, it is a service that ensures that the opponent cannot resend old messages that he may have obtained during the process of transmitting data over the network. means that they are subject to message organizing and will not be resent or reused[10].

4.7. Non-Repudiation

Ensuring that the sensor does not have the ability to disprove send data to the other party or receive data from the other party involved in the communication [12].

4.8. Robustness

In the event of an alteration in the WSN structure such as if new nodes join or several nodes fail, or in the case of a security attack, it must be ensured that the network has a high level of adaptability to changes and reduce the effect of disruption on performance to the lowest level[7]**.**

4.9. Time-Synchronization

The goal of time synchronization is to equivalent the local times of all nodes in the network, if necessary. Because WSNs are limited in computational capability, resources, power, bandwidth, and storage capacity, conventional time synchronization algorithms such as Global Positioning System (GPS) and Network Time Protocol are unpractical for network synchronization[7].

4.10. Secure Localization.

Ensure that the sensor nodes are able to specify their location safely and accurately[13].

4.11. Self-Organization

In the event that a new node is joining or failing some network's nodes, this service guarantees the independence to make coordinates among sensor nodes [14].

V. ATTACKS ON WIRELESS SENSOR NETWORKS

Attacks come in various types against wireless sensor networks. Here we will define the main types of attacks as follows:

5.1. Wormhole attack:

This attack occurs when there are two malicious nodes are far apart and communicate with each other through a tunnel, the first malicious node record packets from its location and forwards them to the second malicious node that restarts them to a different area of the network[15].

5.2. Hello Flood Attack:

A Hello Flood attack is an illegitimate node that broadcasts a high-powered HELLO packet over a large area of the network and it reaches a large number of nodes even far from it. These nodes will assume that this illegitimate node is their neighbor, and these nodes will lose their energy by responding to the HELLO packet.[16].

5.3. Black-hole attack:

Black-hole attacks are malicious nodes that at first pretend to be a component of a good path while the route is detected and once the transmission starts, they reject all packets. Black holes lead to an end-to-end throughput breakdown[17].

5.4. Sinkhole attack:

Attracting traffic in a specific area by means of a malicious knot, which is what the opponent aims at, this will leads to the formation of a metaphorical sinkhole in the center[18].

5.5. Denial of Service attack:

DoS attacks on WSNs are caused by hackers or illegitimate nodes. This attack sends massively wrong requests to block legitimate users from using network resources. It can exhaustion resource usage on the network, increase power consumption and latency, and reduce throughput[19].

5.6. Sybil attack:

Sybil attack in which the attacker fraud other nodes by showing a forged identifier or a duplicate identifier to users that are familiar with the wireless sensor network's nodes[20].

5.7. Attacks against information in transit:

In WSNs, nodes can freely join or quit the network. When the malicious node joins, it will exploit the violations that occur among the network's original nodes, and participate in a data transmission process, after which it will start a message modification attack[21].

5.8. Selective forwarding

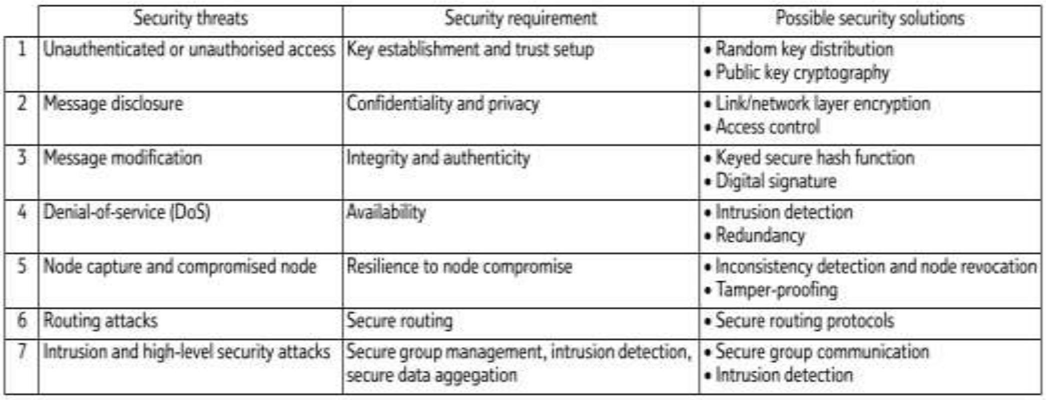
Eachnode in the WSN forwards packets to its neighbors, while in this type of attack, the malicious node doesn't forward all the packets it receives from its neighbors, but drops some packets or ignorance some packet contents, causing the base station to be unable to receive data completely[22].

5.9. Spoofing

Spoofing attacks create when the attacker can root a node on a system to a belief that a part of information came from a source which it really did not start from. Spoofing attacks come in many forms, including IP spoofing, MAC spoofing, email spoofing, web spoofing…etc, [23].

In general, Table(1) below summarizes the threats, related requirements, and possible solutions in a table:

Table(1) of Security threats, Requirements, and potential solutions in the WSNs [24]



	Security threats	Security requirement	Possible security solutions
1	Unauthenticated or unauthorised access	Key establishment and trust setup	• Random key distribution • Public key cryptography
2	Message disclosure	Confidentiality and privacy	• Link/network layer encryption • Access control
3	Message modification	Integrity and authenticity	• Keyed secure hash function • Digital signature
4	Denial-of-service (DoS)	Availability	• Intrusion detection • Redundancy
5	Node capture and compromised node	Resilience to node compromise	• Inconsistency detection and node revocation • Tamper-proofing
6	Routing attacks	Secure routing	• Secure routing protocols
7	Intrusion and high-level security attacks	Secure group management, intrusion detection, secure data aggegation	• Secure group communication • Intrusion detection

VI. SECURITY PROTOCOLS FOR WIRELESS SENSOR NETWORKS

This section contains some types of security protocols for WSNs in different layers:

5.10. Localized Encryption and Authentication Protocol (LEAP)

The LEAP protocol is utilized to equip the Wireless Sensor Network with security and support. It supports a multi-key mechanism, it is also called a Key Management Protocol. LEAP includes: four types of keys (in order to provide different security requirements for messages transmitted between sensor nodes, because a message sent from any sensor node is different from other messages and has different security requirements from the other [25]), RC5 is an encryption algorithm that uses symmetric key block ciphers. It also employs one-way key-chains for broadcast authentication [26].

The four types of keys used in LEAP are [25]:

5.10.1. Individual key:

It's a key that each sensor node shares with its corresponding base station., which provides security during the communication process between them, which is essential because it enables the node to notify the base station when it disclosed any abnormal conduct caused by its surroundings nodes. Therefore, the base station can encrypt important information with the key (information such as instructions to a specific node).

5.10.2. Pairwise Key:

It’s a shared key between each sensor node with its adjacent sensor nodes. This key provides transmission security becauseit is participated between the sensor node and a single of its immediate adjacent nodes, thus preventing intruders. Therefore, it guarantees the protection of communications that require privacy or source authentication. After the individual key is generated, the node sends messages with its ID to its neighbors waiting for a response from them, thus that nodes be able to determine their neighbors.

5.10.3. Group Key:

It's a common key shared by all WSN sensor nodes. It’s else called the Global Key. The base station utilizes this key to encrypt the data it sends to each node inside the group. The message does not need to be encrypted separately with the single key via the base station because the key is shared by all nodes in the group.

5.10.4. Cluster Key:

It's a group key but of a special kind, which is a key that each sensor node shares with several of its neighbor sensor nodes. This key is created by the respective node by utilizing a random function, and with the pairwise key it is encrypted, thus only authenticated neighbors can decrypt the cluster key.

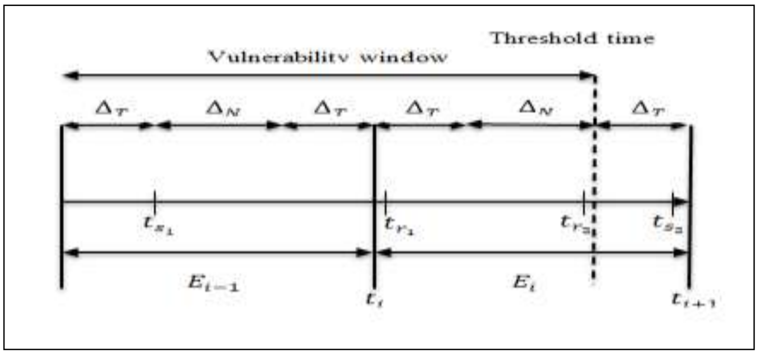
Initially, the individual key is generated by utilizing the function of a seed (pseudo-random function) and the node's ID. Thereafter, the identifiers of the nodes are broadcasted to generate a shared pairwise key and estimate it for the receiving nodes. Next, the cluster head utilizes the pairwise key to scatter the cluster key. Lastly, the group key is spread it at the level of the network by spreading the sink node cluster-by-cluster in a multi-hop method[27].

5.11. MiniSec Protocol

MiniSec is a network layer security architecture, that improves power consumption and increases security. This security protocol optimizes power consumption through two modes: MiniSec-B operates with broadcast communication and MiniSec-U operates with unicast communication.

5.11.1. MiniSec-B works with broadcast mode.

- It uses encryption of Offset Codebook Mode (OCB) to keep the authentication and confidentiality.
- also, a sliding window approach uses, which epoch boundaries are often vulnerable to replay attacks, Figure(2)
- So to handle a vulnerable sliding window, it's enhanced with Bloom filters.
- Thus, in any given epoch the nonce is never reused and the numbers are never wrapped around during the lifetime of a sender, and a receiver keeps Bloom Filters active[28],[29].



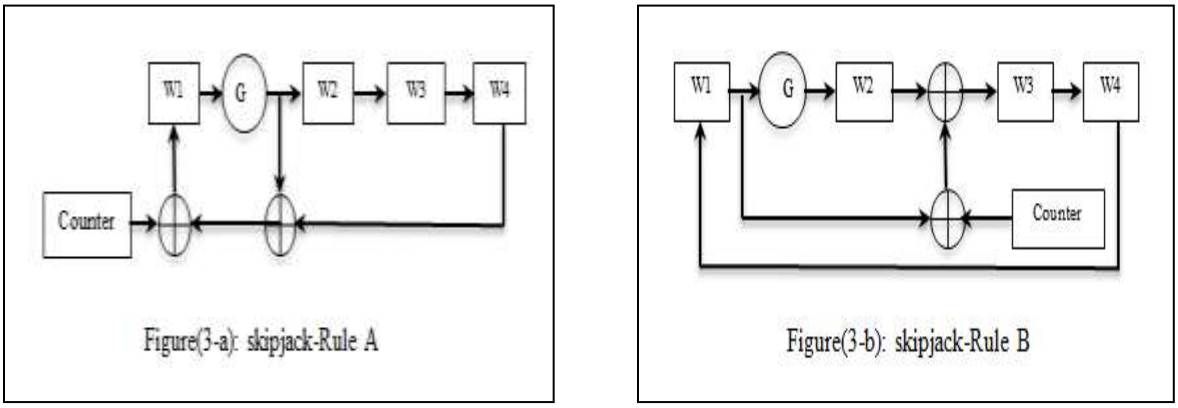
Figure(2): This figure shows the **Timeline** in the sliding window approach.

where the packet received in tr1 cannot be sent before ts2, and the packet received in tr2 can be sent after ts2. Note that ΔN is the maximum network latency, T is the maximum synchronization error between sensor nodes in terms of time, and Ei is the current epoch [29].

6.2.2.MiniSec-Uworks with unicast mode when a packet is sent from the sender to the receiver.

- It utilizes an implied synchronization mechanism to keep the counter incremented monotonously at both the sender and receiver.
- The sender uses the technique of the Last Bit Optimization when it sends a packet with the last 3 bits of its counter attached.
- A receiver will compare the value of the last bits attached with the last 3 bits of its local counter.
- The receiver increments its local counter only if it receives a valid packet and decrypted it.
- Re-synchronization protocol is used to re-synchronize the counters (In crowded channels, counters tend to be de-synchronized).
- It works with OCB encryption which provides confidentiality and authentication.

A skipJack encryption algorithm is used with 64-bits. Because OCB needs the counter to have the same block size as the nonce (64 bits), it can also be resizable depending on what the OCB requires, and although publicly available it is more secure[28].



Figure(3-a): skipjack-Rule A

Figure(3-b): skipjack-Rule B

Figure(3): SKIPJACK Rules, [41].

MiniSec-U keeps a counter for each neighbor with whom it communicates. But this suggestion, if used with the broadcast, will be costly in terms of memory, therefore, for MiniSec-B mode, the authors specify the sliding window technique[28].

5.12. Intrusion tolerant routing protocol (INSENS)

The INSENS protocol is utilizedto prevent attacks and external intrusions, to ensure the integrity of forwarding tables when they are created, and to ensure the authentication of communications. The INSENS protocol has tw]o versions: the first version is known as Basic INSENS, and the second version is known as Enhanced INSENS[30], [31]:

5.12.1. Basic INSENS:

It can be considered as consisting of two phases:

a- Route Discovery Phase.

b- b- Data Forwarding Phase

a- Route Discovery phase :

In the Route Discovery phase, all the information on the topology is got and convenient forward tables are created for each node. It includes three stages:

1-Route Request. 2-Route Feedback. 3-Computing and Propagating Multi-path Routing Tables.

1- Initially (or if the topology of the network is altered), the base station floods all network nodes with the request message REQ.

2- When node x receives a REQ message, it broadcasts feedback that contains the receives another REQ message, it registers the sender as a neighbor but will not return to broadcast a feedback message for that repeat request.

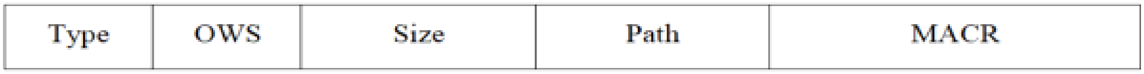
3- The feedback messages are authenticated by the BS that received them from the nodes, builds a network topology image from the neighborhood information which is authenticated, calculates the redirection tables for every node, and then, via a Routing Update message, these tables are sent to the nodes consecutively.

b- Data Forwarding Phase

This phase is purely able to forward data from all nodes to the base station and back. It should be noted that all communicationsamong nodes are forwarded in one direction (unicast) through the base station BS.

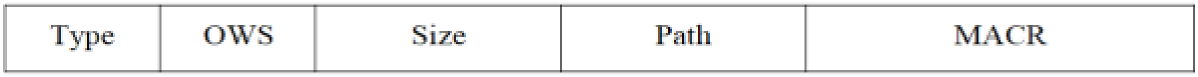
The essential concept of this protocol is to add fields into the message that support INSENS' intrusion-tolerant features, which are the One-Way Sequences field 'OWS' and the Message Authentication Code Request/Feedback field'MAC' (MACR/MACF).

REQ/Feedback messages format consists of the following fields: **Type** the type of the message(request, feedback, routing, or data message), **OWS** One-Way Sequence, **Size** the length of this path, **Path**the route between the base station and the present node which sends the request message, **MACR** Message Authentication Code Request, **Parent-info** determines the parent of the node, **nbr info**list of neighbors, and **MACF** Message Authentication Code Feedback, Figure(4).



Type	OWS	Size	Path	MACR

Figure (4-a): REQ message format



Type	OWS	Size	Path	MACR

Figure (4-b): Feedback message format

Figure (4): The format of the REQ message and the Feedback message for the basic INSENS protocol [30].

5.12.2. Enhanced INSENS

This version uses Global Key GK, Pairwise Key PK, and Cluster Key CK to confirm the neighboring node so that the protocol can prevent malicious nodes from intrusion or snooping. It works in essential four phases as follows [32], [33]:

- Echo phase. - Key Exchange phase.
- Route Requests phase. - Setup phase.

a- Initially, INSENS protocol injects a GK to every node in the network before scattering them to prevent external intrusion.

b- **Echo phase:** An encrypted message is used which utilizes the pre-injected GK to prevent intrusion from an external node. An echo message is created using GK at each node and then broadcast. When a neighboring node receives the echo message, it uses GK to ensure that the received message is valid, then each node generates a PK with the node from which the echo message was received. Then, the node broadcasts an echo-back message after the PK is included in it.

c- **Key Exchange phase:** At this phase, each node generates a CK and forwards it to each neighbor node using its own PK with each of these neighbor nodes.

d- **Route-Request phase:** At this point, the BS uses its own CK to generate a REQ message in order to prepare a routing path setup.

e- **Setup phase:** After that, BS broadcasts the REQ message so as to set up the routing path, and also it increases the value of OHC by 1.

f- Neighbor nodes that receive the REQ message use the sender node's CK and their OHC to authenticate the message.

g- After the nodes have authenticated the REQ messages, each node will use its own CK to broadcast an encrypted REQ message, and then increase the value of its own OHC by 1.

h- The WSNs iterate these procedures so as to form the routing path.

6.4.Security Protocols for Sensor Networks (SPINS) Protocol

SNIPS protocol is designed to protect two kinds of communications in WSNs, as follows [34]:

a. Unicast communications :

Communication from the Base Station to the sensor node (e.g., certain requests), or from the sensor node to the Base Station (e.g., sensor readings) are unicast types of communication between a Base Station and a particular sensor node. For securing these unicast communications the **SNEP** is designed.

b. Multicast communications:

From Base Station to each node (e.g., re-programming of the whole network or queries) one to many multicast communications are a necessity.**µTESLA** is used for securing multicast communications in WSNs.

SPINSinvolves two suits of security protocols for securing communications of wireless sensor networks, these two protocols are SNEP and μTESLA.

6.4.1 SNEP:

The Sensor Network Encryption Protocol (**SNEP**) is basically providing authentication between two nodes, confidentiality, the freshness of weak messages, and data integrity in a WSN. Maintaining data encryption is one method of data confidentiality but this is not considered pure data security, so a Semantic Security feature is used. And a Message Authentication Code (MAC) is used to obtain the message's integrity and authenticity.
The base station and the sensor nodes should be inaccurately time-synchronized, and every node must know the upper limit of the maximum time-synchronization error. This is what is necessary for Tesla [6].

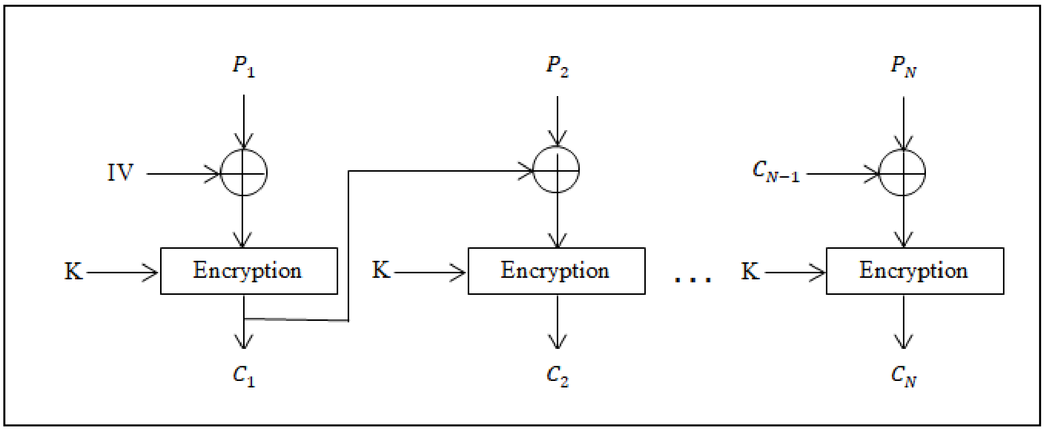
6.4.2. The Micro TESLA:

μTESLA protocol generates a MAC key (by the MAC algorithm), broadcasts a packet authenticated with a MAC key first, then propagates the key so that the broadcast packet cannot be falsified before the key is published. This protocol also performs secret sharing by utilizing a network-wide key-generation algorithm. Key integrity and packet loss tolerance can be assured through a one-wayhash function and a key-chain mechanism [35]**.**

6.5. TINYSEC protocol

In a Wireless Sensor Network, the link-layer security protocol is fully implemented. All communications are authenticated and encrypted by software without the use of any specialized hardware. In order to realize authentication and integrity, it relies on Message Authentication Code (MAC).Furthermore, TinySec is based on the cipher scheme, which is the CBC Cipher Block Chaining.And the best cipher algorithm used with TinySec is Skipjack. Furthermore, be aware that to make a contrast in the cipher, an IV should be used with it, essentially with few or no differences between messages[36], as shown in Figure(5).

Since it is necessary for each security protocol to present integrity and authenticity. Therefore, TinySec calculates and validates MACs relying on CBC-MAC. And also, MAC length affects the execution of CBC-MAC. TinySec uses a MAC with 4bytes, therefore the opponent has 2^{32} possibilities to detect a true MAC. For any security protocol, it needs to have a counter with 8 bytes and an IV with 16 bytes to prevent redundancy, but in TinySec due to resource constraints, it only has a 2-byte counter and 8-byte IV. The counter supplies the variance to the IV, and the IV affects the encryption algorithm. So, in a counter with 2 bytes, the IV will be reused only after 2^{16} packets have been sent [36].



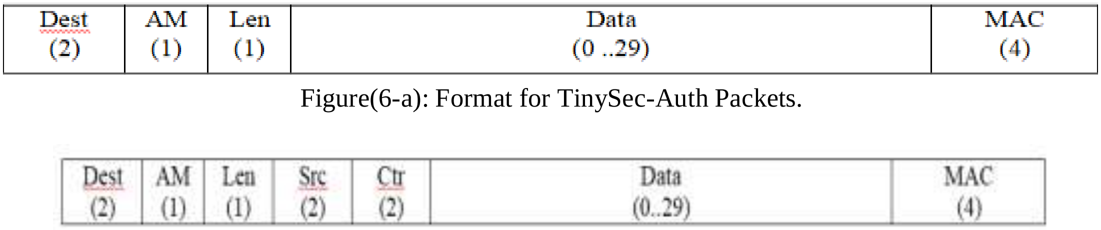
Figure(5) : CBC Encryption scheme[36]

There are two security choices supported by TinySec, and they are as follows [36]:

- Authentication only **(TinySec-Auth)**, which just authenticates the packet and does not encrypt the payload.
- Authenticated Encryption **(TinySec-AE)** which performs packet authentication and payload encryption.

In TinySec-AE, packet latency increases more than packet latency increases in TinySec-Auth[36]. Figure (6) shows TinySec packet formats.

Only at the final destination, if the integrity of the message is verified, the packets that were injected by the opponent are then may rout by the network. When unauthorized packets are first entered into the network, the architecture of the link-layer security can find these packets and not wait until they reach the final destination[37].



Dest (2)	AM (1)	Len (1)	Data (0 ..29)	MAC (4)

Figure(6-a): Format for TinySec-Auth Packets.

Dest (2)	AM (1)	Len (1)	Src (2)	Ctr (2)	Data (0..29)	MAC (4)

Figure(6-b): Format for TinySec-AE Packets.

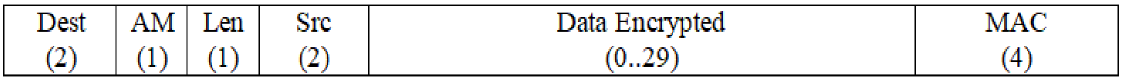
Figure (6): TinySec-Auth 37-bytes Packet Format, TinySec-AE 41_bytes Packet Format, [38].

6.6. Link-Layer Security Protocol (LLSP)

For WSNs, LLSP is a secure link-layer architecture.By implementing replay protection, LLSP conquers TinySec's security vulnerabilities. It uses AES-CBC mode for the confidentiality of a message, and CBC-MAC for integrity and authentication of a message. The MAC value is created based on encrypted data and Initial Vector IV. The IV is created as below[39]:

$IV_{LLSP} = Dest_2 \parallel AM_1 \parallel Len_1 \parallel Src_2 \parallel Ctr_4$

To guarantee replay protection, the LLSP uses a synchronous counter of 4bytes between the sender's node and the receiver's node, also it uses Feedback Shift Register (FSR) for updating this counter. This counter must be kept in sync between the sender and receiver. Therefore, it does not need to send the value of the counter. Thus, the counter bits are discarded from the packets, Figure(7) shows the packet format[40].



Dest (2)	AM (1)	Len (1)	Src (2)	Data Encrypted (0..29)	MAC (4)

Figure(7): LLSP Packet Formats [40]

VII. CONCLUSION:

Recently, WSNs have become the focus of attention of researchers and developers due to their importance and expansion in many areas such as medical applications, military, environmental disasters...etc. Some of these applications need more security and confidentiality than others, but because the wireless infrastructure is limited in resources, this results in a lower level of security in the network. Therefore, the need arose for new protocols that provide a good level of security for the network and its connections, despite the limited resources.

This paper summarized the different attacks on WSN and the different protocols for WSN security to show the strength and limitations of each security protocol. This will go to handle, to help the process of choice of security protocol to be implemented in various applications.

REFERENCES

[1] A. Dumka, S. K. Chaurasiya, A. Biswas, and H. L. Mandoria, A Complete Guide to Wireless Sensor Networks From Inception to Current Trends. CRC Press, 2019.

[2] D. E. Boubiche, S. Athmani, S. Boubiche, and H. Toral-Cruz, Cybersecurity Issues in Wireless Sensor Networks: Current Challenges and Solutions, vol. 117, no. 1. Springer US, 2021.

[3] A. Karakaya and S. Akleylek, “A survey on security threats and authentication approaches in wireless sensor networks,” 6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding, vol. 2018-Janua, pp. 1–4, 2018, doi: 10.1109/ISDFS.2018.8355381.

[4] S. Youn, “Analysis of security protocols in wireless sensor networks,” ICIC Express Lett. Part B Appl., vol. 11, no. 11, pp. 1087–1093, 2020, doi: 10.24507/icicelb.11.11.1087.

[5] Y. A. Bangash, Q. ud D. Abid, A. Alshreef Abed Ali, and Y. E. A. Al-Salhi, “Security issues and challenges in Wireless Sensor Networks: A survey,” IAENG Int. J. Comput. Sci., vol. 44, no. 2, pp. 135–149,

2017, doi: 10.17148/IJARCCE.2020.9140.

[6] A. Perrig et al., “SPINS: Security Protocols for Sensor Networks SPINS : Security Protocols for Sensor Networks,” Wirel. Networks, vol. 8, no. September, pp. 521–534, 2009.

[7] P. Pathak, “Issues , Challenges and Solution for Security in Wireless Sensor Networks : A Review,” Int. J. Electr., 2017, [Online]. Available: www.researchtrend.net.

[8] M Bhalla, N Pandey, and B Kumar, “Security Protocols for Wireless Sensor Networks,” in Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) 8-10 October 2015, Greater Noida, India : venue: GCET, Greater Noida, Delhi, 2015.

[9] P. Kumar and H. J. Lee, “Security issues in healthcare applications using wireless medical sensor networks: A survey,” Sensors, vol. 12, no. 1. pp. 55–91, 2012, doi: 10.3390/s120100055.

[10] A. Jain, K. Kant, and M. R. Tripathy, “Security solutions for wireless sensor networks,” in Proceedings - 2012 2nd International Conference on Advanced Computing and Communication Technologies, ACCT 2012, 2012, pp. 430–433, doi: 10.1109/ACCT.2012.102.

[11] M. Keerthika and D. Shanmugapriya, “Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures,” Glob. Transitions Proc., vol. 2, no. 2, pp. 362–367, 2021, doi: 10.1016/j.gltp.2021.08.045.

[12] A. S. Uluagac, C. P. Lee, R. A. Beyah, and J. A. Copeland, “Designing secure protocols for wireless sensor networks,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2008, vol. 5258 LNCS, pp. 503–514, doi: 10.1007/978-3-540-88582-5_47.

[13] S. Saleem, S. Ullah, and K. S. Kwak, “A study of IEEE 802.15.4 security framework for wireless body area networks,” Sensors, vol. 11, no. 2, pp. 1383–1395, 2011, doi: 10.3390/s110201383.

[14] J. Shahid and S. Saleem, “Dos Attacks on Wsn and Their Classifications With Countermeasures - a Survey,” NUST J. Eng. Sci., vol. 9, no. 2, pp. 50–59, 2016.

[15] M. M. Patel and A. Aggarwal, “Two phase wormhole detection approach for dynamic wireless sensor networks,” in Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016, 2016, pp. 2109–2112, doi: 10.1109/WiSPNET.2016.7566514.

[16] A. Dubey, D. Meena, and S. Gaur, “A Survey in Hello Flood Attack in Wireless Sensor Networks,” vol. 3, no. 1, pp. 1882–1888, 2014, [Online]. Available: www.ijert.org.

[17] S. D. Roy, S. A. Singh, S. Choudhury, and N. C. Debnath, “Countering sinkhole and black hole attacks on sensor networks using dynamic trust management,” in Proceedings - IEEE Symposium on Computers and Communications, 2008, pp. 537–542, doi: 10.1109/ISCC.2008.4625768.

[18] J. Qi, T. Hong, X. Kuang, and L. Qiang, “Detection and defence of Sinkhole attack in Wireless Sensor Network,” in International Conference on Communication Technology Proceedings, ICCT, 2012, pp. 809–813, doi: 10.1109/ICCT.2012.6511315.

[19] M. T. Kurniawan and S. Yazid, “Mitigation and Detection Strategy of DoS Attack on Wireless Sensor Network Using Blocking Approach and Intrusion Detection System,” 2020, doi: 10.1109/ICECCE49384.2020.9179255.

[20] R. Lakhanpal and S. Sharma, “Detection &Prevention of Sybil attack in Ad hoc network using hybrid MAP & MAC technique,” 2016, doi: 10.1109/ICCPEIC.2016.7557211.

[21] A. L. Gupta, Sunil; Verma, Harsh K.; Sangal, “Security Attacks &amp; Prerequisite for Wireless Sensor Networks,” Int. J. Eng. Adv. Technol., vol. 2, no. 5, p. 9, 2013, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.676.238&rep=rep1&type=pdf.

[22] D. Y. Zhang, C. Xu, and L. Siyuan, “Detecting selective forwarding attacks in WSNs using watermark,” 2011, doi: 10.1109/WCSP.2011.6096939.

[23] K. Jindal, S. Dalal, and K. K. Sharma, “Analyzing spoofing attacks in wireless networks,” in International Conference on Advanced Computing and Communication Technologies, ACCT, 2014, pp. 398–402, doi: 10.1109/ACCT.2014.46.

[24] H. S. Ng, M. L. Sim, and C. M. Tan, “Security issues of wireless sensor networks in healthcare applications,” BT Technol. J., vol. 24, no. 2, pp. 138–144, 2006, doi:

10.1007/s10550-006-0051-8.

[25] J. R. Arunkumar and M. R. Prabhu, “Lightweight Extensible Authentication Protocol Based Wireless Sensor Network,” vol. 7, no. 10, pp. 66–74, 2017, doi: 10.9790/9622-0710056674.

[26] A. Tiwari, R. Verma, M. M. S. Rauthan, and V. Barthwal, “Analysis of security attacks and security protocols of wireless sensor network: Review,” Int. J. Sci. Technol. Res., vol. 9, no. 1, pp. 3270–3277, 2020.

[27] S. R. Rajeswari and V. Seenivasagam, “Comparative Study on Various Authentication Protocols in Wireless Sensor Networks,” Scientific World Journal, vol. 2016, no. iii. 2016, doi: 10.1155/2016/6854303.

[28] V. Bhasin, S. Kumar, P. C. Saxena, and C. P. Katti, “Security architectures in wireless sensor network,” Int. J. Inf. Technol., 2020, doi: 10.1007/s41870-018-0103-6.

[29] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, “MiniSec: A secure sensor network communication architecture,” IPSN 2007 Proc. Sixth Int. Symp. Inf. Process. Sens. Networks, pp. 479–488, 2007, doi: 10.1145/1236360.1236421.

[30] V. H. La and A. R. Cavalli, “A Comparative Evaluation of Two Intrusion-Tolerant Routing Protocols for Wireless Sensor Networks,” Proc. - 2015 10th Int. Conf. Broadband Wirel. Comput. Commun. Appl. BWCCA 2015, pp. 6–12, 2015, doi: 10.1109/BWCCA.2015.104.

[31] V. H. La and A. Cavalli, “A study of Intrusion-tolerant routing in Wireless Sensor Networks,” Proc. Inst. Syst. Program. RAS, vol. 26, no. 6, pp. 99–110, 2014, doi: 10.15514/ispras-2014-26(6)-9.

[32] K. Song and T. Cho, “An Energy-Efficient Method for Preventing Internal Sinkhole Attacks on INSENS based WSNs using Interactive Authentications,” Int. J. Comput. Appl., vol. 153, no. 2, pp. 38–44, 2016, doi: 10.5120/ijca2016911978.

[33] M. Karpagam, “Heed Protocol Using A Cluster Based V2V Communication,” Indian J. Sci. Technol., vol. 12, no. 6, pp. 1–7, 2019, doi: 10.17485/ijst/2019/v12i6/141891.

[34] S. Islam, “Security property validation of the sensor network encryption protocol (Snep),” Computers, vol. 4, no. 3, pp. 215–233, 2015, doi: 10.3390/computers4030215.

[35] H. Huang, T. Gong, T. Chen, M. Xiong, X. Pan, and T. Dai, “An Improved µ TESLA Protocol Based on Queuing Theory and Benaloh-Leichter SSS in WSNs,” J. Sensors, vol. 2016, 2016, doi: 10.1155/2016/9021650.

[36] S. M. Almheiri and H. S. Alqamzi, “Data link layer security protocols in Wireless Sensor Networks: A survey,” 2013 10th IEEE Int. Conf. Networking, Sens. Control. ICNSC 2013, pp. 312–317, 2013, doi: 10.1109/ICNSC.2013.6548756.

[37] B. Mbarek and A. Meddeb, “Energy efficient security protocols for wireless sensor networks : SPINS vs TinySec,” 2016 Int. Symp. Networks, Comput. Commun. ISNCC 2016, 2016, doi: 10.1109/ISNCC.2016.7746117.

[38] C. Karlof, N. Sastry, and D. Wagner, “TinySec: A link layer security architecture for wireless sensor networks,” SenSys’04 - Proc. Second Int. Conf. Embed. Networked Sens. Syst., pp. 162–175, 2004.

[39] S. Mondal, S. K. Mohanty, and S. Nandi, “Energy efficient secure communication architecture for wireless sensor network,” Secur. Commun. Networks, vol. 9, no. 16, pp. 3314–3323, Nov. 2016, doi: 10.1002/SEC.1536.

[40] S. In et al., “a Model for Selecting Security Protocols Fulfillment of the Requirements for the Award of,” 2013.

[41] Z. Azri, B. Muhamad, M. A. Algaet, and U. Teknikal, “Comparative Study of Performance in Cryptography Algorithms (Blowfish and Skipjack) Ali Ahmad Milad , 2 Hjh Zaiton Muda , Department of Computer System and Communication , Department of Computer Science ,” vol. 8, no. 7, pp. 1191–1197, 2012.