Engineering and Technology Journal e-ISSN: 2456-3358

Volume 09 Issue 02 February-2024, Page No.-3503-3508

DOI: 10.47191/etj/v9i02.09, I.F. – 8.227

The Network Security in Wireless Sensor Networks: A Review

Dinesh Kumar Gupta[1], Dr. Deepika Pathak[2]

[1,2] Department of Computer Application, Dr. APJ Abdul Kalam University, Indore (M.P.) India

ABSTRACT: Wireless Sensor Networks (WSN) is an innovative technology predicts to be used ever more in the next to future due to their data achievement and data processing capability. Security for WSN requires to be considered in order to defend the functionality of this network such as the information it communicate and the position of nodes. The safety models & protocols used in traditional networks are not appropriate to WSNs because of its limited resource constraints.

KEYWORDS: WSN, Network Security, Protection, Safety, Attack, Threats.

1. INTRODUCTION: WIRELESS SENSOR NETWORK

A wireless sensor network is basically described as a huge group of sensor nodes, each prepared with its individual sensor, processor and radio transceiver. Such networks have important data achievement and data processing facility. This network is deployed compactly throughout the region where it will monitor specific occurrence. However, due to the lack of insecure nature of wireless communication media, WSN is unsafe to internal and external attacks.

Attack and attacker are the mainly ordinary terms used in the protection. Attacker is an illegal to access the information of the system or tries to give the wrong impression about the information. When an attacker rights to use the services of the network system then it is identified as attack.

Safety in the Wireless Sensor Networks has a variety of difficulties, such as dynamically varying topology, wireless communication along with the sensor nodes, framework without infrastructure and partial physical resources like power source, memory capability and small communication bandwidth. Various analysts proposed a lot of threats managing models and different security protocols for safe data communication and routing in WSN [1].

WSN is used in several applications from inside to outside. Even as transmitting message in the network, it is essential to give security. Security is measured to be the mainly demanding task in WSN. It's hard to maintain observe on the sensor network every time. But it should be protected to prevent an attacker from attacking the broadcast of information [2].

2. WSN STRUCTURE

The main components of a classic WSN are: Sensors, Sensing Range, Sink Node and Base Station, as shown in Figure 1.

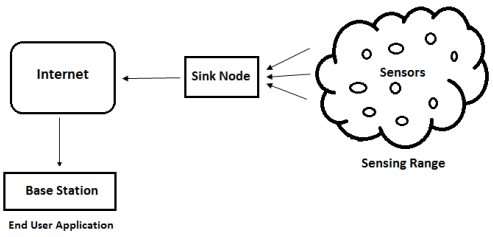

Figure 1: WSN Communication Structure

We define these components as follows;

2.1. Sensing Range: A sensing range can be considered as an area in which the nodes are located, where a particular event to occur.

2.2. Sensors: Sensor nodes or motes are the main part of the network. They collect the data and route this information to the sink.

2.3. Sink Node: A sink node is a sensor node with the specific job of receiving, processing and storing data from the other sensor nodes.

2.4. Task Manager or Base Station: It is a centralized position of control within the network, which extracts the information from the network and distributes control information back to the network. It also considers as a gateway to other networks. It's a powerful data processing and storage centre and an access point for a user interface. The base station is either a laptop computer or a workstation. Data is collected from these

workstations either via the internet, wireless channels, satellite etc.

So, many nodes are deployed in a sensing range to create a wireless sensor network. Nodes can use wireless communication media such as infrared, radio, fiber optical media or blue-tooth for their communications. The communication range of the sensor nodes varies according to the used communication protocol.

3. SECURITY REQUIREMENTS

WSNs have to accomplish some requirements for giving a safe communication. Basic security necessities of WSNs are confidentiality, integrity, authentication and availability, [3][4]. Some additional requirements known as minor requirements are source localization, self organization and data freshness [5][6][7]. These requirements provide defense against attacks to the information transmitted over the WSN [8].

3.1. Confidentiality: Defending the important information from unauthorized access. In WSN, information flows from numerous intermediate nodes and possibility of data disclose is more [9]. To give the data confidentiality, an encrypted data is sent by sender so that only receiver decrypts the data to its original form.

3.2. Integrity: Keep the uniqueness of the information. Data received by the receiver should not be distorted or modified by anyone, is Data Integrity. Original data is altered by attacker due to insensitive environment. The attacker may modify the information according to its need and sends this new information to the recipient [10].

3.3. Authentication: It is the method of verification that the communicating node is the authentic node. It is essential for receiver node to do confirmation that the information is received from a validate node. Authentication ensures that the communicate node is authentic node.

3.4. Availability: It allows access to the available data. Data Availability means that the services are accessible all the time still in case of some attacks like DOS (Denial of service).

Unavailability of sensor nodes can happen in case of hardware breakdown when the sensor's battery power is very low due to overload computation or communication. In other cases, it can happen that an attacker can squash message to create sensor unavailable.

3.5. Source Localization: In data communication, some applications make use of location information of the sink node. It is essential to provide safety to the location information. Non-secured node can be controlled by the malicious node by sending false signals or replaying signals.

3.6. Self-Organization: In WSN, no predetermined network topology exists. Therefore, every node is having self-determining properties of adaptation to the dissimilar situations and maintains self organizing and self remedial properties. It is a big challenge for safety in WSN.

3.7. Data Freshness: Data freshness defines that every message transmitted over the transmission media is fresh and new. It assures that the old information cannot be replayed by any node. It can be solved by implementing some time associated counters to verify the freshness of the information.

4. SECURITY CLASSES

The network attacks can be generally classified as interruption, interception, modification and fabrication. [11][12]

4.1. Interruption: The attack on the availability of the network is identified as Interruption.

4.2. Interception: The attack on confidentiality is identified as Interception. The WSN can be co-operated by an attacker to achieve unauthorized access to sensor node or data stored within it.

4.3. Modification: The attack on integrity is identified as Modification. Modification defines that an unauthorized user not only accesses the data but alters it.

4.4. Fabrication: The attack on authentication is identified as Fabrication. Fabrication defines that an attacker injects fake data and compromises the consistency of the information transmitted.

5. CLASSIFICATION OF SECURITY THREATS

WSNs are weak against numerous attacks. Attackers can hit the radio transmission; append their personal data bits to the media, repeat old packets and any additional type of attack. A protected network should be hold all security properties [13][14]. Attackers can set up some malicious nodes in the network with related capabilities as of normal node. It can also overwrite the memory of normal organized node by capturing them. The Attacks in WSNs are shown in Figure 2.

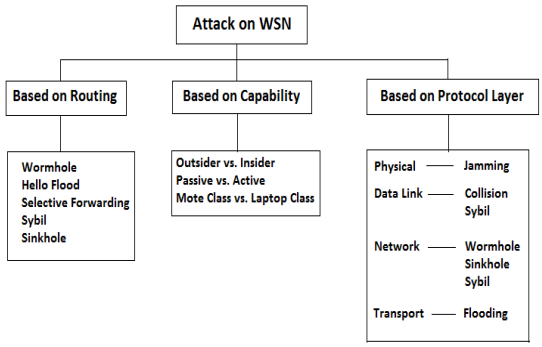

Figure 2: Attacks in WSN

5.1. On the Basis of Routing

There are many routing protocols planned for transmitting the information in the network from source to sink node. An attacker can take or modify the data with the help of unusual attacks in this transmission process [12][15]. A few routing attacks are described below:

(a) Wormhole Attacks

In wormhole attack, two or more malicious nodes are present in the network at dissimilar locations. When sender node sends information, then a malicious node forwards this information to a further malicious node. After that the receiving malicious node sends this information to its nearby nodes. In this manner, attacker prove to the sender and receiver nodes that they are located at short distance of one or two nodes but real distance between these two nodes are multiple points and frequently both are out of range.

(b) HELLO Flood Attacks

In a WSN, to find out the neighbors, a HELLO message broadcasts by the sender nodes. The recipient node considers that the source node is in the range of network and sends its sensed information to the announcer. In this Attack, a message 'HELLO' is broadcast with high spread power by the attacker [16]. The nodes receive this HELLO message and send the information to the attacker node. Attacker can modify this information or drop it. In this method, large amount of energy is wasted and network overcrowding occurs also.

(c) Selective Forward Attack

In selective forward attack, a malicious node break off the communication process in the network. So, multiple malicious nodes that depend upon the attacker can interrupt the communication process in the network [17]. This node selectively forwards a number of the received data packets. If this malicious node drops all the received packets then it is referred as a black hole. In this case, adjacent nodes suppose that it is failed and it again starts searching for other route. If it acts as a black hole and drops all the received data packets then this attack is easy to detect but if it forwards packet selectively then it is complicated to detect.

(d) Sybil Attack

In Sybil Attack, a single attacker creates and shows dissimilar identities to the other nodes in the network. It can be measured as "Node can be in more than one place at once". The malicious node is known as Sybil node. This attack is applied against redundancy method of distributed systems. In WSNs, this attack is usually used to attack some types of protocols. It is a serious risk to a location based protocols in which location information is switched for proficient routing [18].

(e) Sinkhole Attack

In sinkhole attack, the malicious node announces false routing information to catch the attention of the network traffic [5]. WSN is at risk to this type of attack because communication occurs in many to one form.

5.2. Based on Capability

The stage of information access and its harm is dissimilar, depending upon the category of attack [19]. On the base of capability, attacks are categorized as follows:

(a) Outsider vs. Insider Attacks

In **Outside attack**, the attacker finds an unexpected access of the organized network from outside and wants to damage the network. It is also identified as an external attack. The attacker nodes which involve and perform this type of attack are not the element of network but authorize to damage the network.

In **Inside attack**, an authorized node located in the network is malicious. These attacks are created from inside nodes in the network rather than from outside node. Harmful nodes are really an element of the network system. Inside attacks are more risky than outside attacks because the insider knows important information and have every kind of access permissions.

(b) Passive vs. Active Attacks

These attacks are separated on the base of stage of damage or point at which attacker can right to use the network.

In **passive attacks**, Interruption is not occurred in the authentic communication. An attacker can watch the traffic and access the data without altering it. The attacker collects only the sensitive data. Interception, traffic watching and testing are the examples of it. In this attack, the hacker continuously monitors the network to get the precious information through unlock ports. The attacker does not try to create changes in data.

In **active attacks**, the attacker interrupts the authentic communication by altering the data. Attacker can append some defective data in the real data stream. This attack affects the performance of the network. Denial of Service (DOS), copy, alteration and message repeat are the examples of it. In this attack, a hacker attempts to attack data while data is sent to some other place. Attacker can create changes in data or can hack secret information while data is transferred [20].

(c) Mote-class vs. Laptop-class Attacks

In **mote-class attacks**, an attacker attacks some nodes with the same functions as the normal network node. The attacker has at least one approved node in the network to take the key or code. Therefore, it is also identified as inside attack.

In **laptop-class attack,** the attacker does not have any particular access to the network. An attacker has extra effectual and commanding devices having extra battery power, controlling radio transmission, extra able CPU, sensitive antenna etc for monitoring the network. These are also identified as outside attacks. For example: laptop and its equivalent devices. It can make extra harm to a network in comparison to a normal malicious node. A regular node may just have the ability to upset its nearby network, while a laptop class attacker may have

the ability to disturb the entire network with utilizing its powerful transmitter.

5.3. Based on Protocol Layer

The WSN is separated into protocol layers. The functioning of each layer is singular. The attacks on the base of protocol layers are as follows [3].

(a) Physical Layer

Physical layer is utilized for convey information in rare bits over the wire or wireless media. It is simple to stuff a general radio signals. Basically, physical layer attacks are classified as Eavesdropping, Tampering and blocking [21]. In eavesdropping attack, an unofficial receiver reads the information. Tampering is the obstruction with the radio frequency used by the nodes in the network. This entirely changes the functioning of network. Blocking attack implements in denial-of-service (DoS) attack.

(b) Data Link Layer

Data link layer is used to ensure the appropriate communication on the physical layer between nodes. This layer achieves error detection, multiplexing, repeated broadcast, collision avoidance and so on. Data Link layer attacks include collisions, cross-talk, and packet repeat. Error detection and correcting codes can be applied to reduce the number of collisions but due to this the routing overload is increased in the network. Another attack is the denial-of-sleep (DoSL) attack, in which node is not capable to go to the sleep mode. This decreases the entire network lifetime.

(c) Network Layer

Network layer is answerable for the data routing among nodes, nodes to sink, nodes to base station [18][5]. The attacker performs a direct attack on routing protocols. It can have collision on network data traffic; destroy messages into the data path between the source and destination. This assumes that effectual and authoritative routing protocols are required to control node failure and attacks on security. Some network layer attacks include wormhole attacks, selective forwarding, spoofing, and black holes.

(d) Transport Layer

Transport Layer is used to make up a communication link for outer network connected with the internet [4]. The attacks of transport layer protocols are de-synchronization and flooding. In the de-synchronization attack, the attacker node copy the packets to at least one or both ends of a link using dissimilar sequence numbers on the packets. In this mode, host needs for re-transmission of the missed packets. In the flooding attack, the attacker reduces the node's memory by sending frequent requests for connection establishment.

6. SAFETY PROTOCOLS IN WSN

The Cryptography is a fundamental technique to accomplish the safety in a network. It establishes a safe connection between two end points. In this method, sender encrypts the original message and receiver decrypts the received message to get the original message.

Different kinds of keys are used in the procedure of cryptography. A variety of protocols are planned by many authors for solving the safety matter in WSN are [14]:

6.1. SPIN

SPIN (Sensor Protocols for Information via Negotiation) protocol performs in three steps. First, a node advertises the ADV packet including the data. Second, if the received node is required the data then it sends the request for data using REQ packet. Finally, after receiving request, the advertiser node sends the DATA packet to the requestor node. It works best in small size networks because of its effectiveness and high latency property [22].

6.2. LEAP

LEAP (Localized Encryption and Authentication Protocol) is a protocol with key management method that is extremely well-organized with its safety system used for large scale distributed network. Generally it supports for inside network processing like data aggregation. In network processing results, it reduces the energy spending in network. It gives the confidentiality and authentication to the data packets. LEAP is suitable for numerous security and performance needs of WSN. LEAP is applied to protect against Wormhole Attack, HELLO Floods Attack, and Sybil Attack [6].

6.3 TINYSEC

TINYSEC is data link layer security design for WSN. It is a trivial protocol. It supports confidentiality, authentication and integrity. To get confidentiality, encryption is made by using CBC (Cipher-block chaining) mode with cipher text, and authentication is made using CBC-MAC. TINYSEC has no counters. Therefore, it doesn't ensure the data freshness. Certified senders and receivers distribute a secret key to calculate a MAC [8].

6.4. ZIGBEE

ZIGBEE is a classic wireless communication technique. It is used in a variety of applications such as environment monitoring, home automation etc. The IEEE 802.15.4 standard is used for ZIGBEE. It holds data confidentiality and integrity. To apply the security method, it uses 128 bit keys. A trust center is used in it, which validates and allows other devices and nodes to connect the network and allocate the keys also [9].

7. INTRUSION DETECTION SYSTEM (IDS)

Intrusion Detection Systems (IDSs) are able to query the status of the network by receiving data about inside events. They operate by collecting and analyzing the data in order to notice attacks and apply the proper countermeasures. IDSs are able to recognize both inside attacks and outside attacks happening in the network [23][24][25].

8. CONCLUSION

Wireless Sensor Networks are resource restricted. They are organized densely (compactly). They are able to failures due to battery power down. The number of nodes in WSNs is in several orders and scattered anywhere in sensing range. WSN network topology is continuously varying. WSNs use a broadcast transmission media and sensor nodes don't have universal naming tags. WSN is a special type of network and shares some common things with a classic computer network. The safety services in a WSN should defend the information transmitted over the network, the resources from attacks and misconduct of sensor nodes.

REFERENCES

1. Grover J. & Sharma S. (2016). Security Issues in Wireless Sensor Network – A Review. 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Sep. 7-9, 2016, AIIT, Amity University Uttar Pradesh, Noida, India, 397-404.
2. Roman R., Zhou J. & Lopez J. (2005). The Security of Wireless Sensor Networks. International Conference on Computational Science and Its Applications – ICCSA 2005, May 9-12, 2005, Springer Verlag, Heidelberg, Germany, 681–690.
3. Pandey A. & Tripathi R.C. (2010). A survey on Wireless Sensor Networks Security. *International Journal of Computer Applications*, 3(2), 43-49.
4. Aseri T. C. & Singla N. (2011). Enhanced Security Protocol in Wireless Sensor Networks. *International Journal of Computers, Communications & Control*, 6(2), 214-221.
5. Ahlawat J., Chawla M. & Sharma K. (2012). Attacks and Countermeasures in Wireless Sensor Network. *International Journal of Computer Science and Communication Engineering (IJCSCE)*, 66-69.
6. Modares H., Salleh R. & Moravejosharieh A. (2011). Overview of Security Issues in Wireless Sensor Networks. Third International Conference on Computational Intelligence, Modelling & Simulation, Langkawi, 308-311
7. Padmavathi G. & Shanmugapriya D. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. *International Journal of Computer Science and Information Security (IJCSIS)*, 4(2), 1-9.
8. Zhu S., Setia S. & Jajodia S. (2010). LEAP: Efficient Security Mechanisms for Large Scale Distributed Sensor Networks. 10th ACM Conference on Computer and Communications Security (CCS 03), 62-72.
9. He D., Chan S., Guizani M., Yang H. & Zhou B. (2014). Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems*, 26(4), 1129- 1139.
10. Ghormare S. & Sahare V. (2015). Implementation of data confidentiality for providing high security in Wireless Sensor Network. International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 1-5.
11. Karlof C., Sastry N., & Wagner D. (2004). Tinysec: A link layer security architecture for wireless sensor networks. SenSys'04 - Proceedings of the Second International Conference on Embedded Networked Sensor Systems, Nov 3-5, 2004, 162–175.
12. Sharif L. & Ahmed M. (2010). The Wormhole Routing Attack in Wireless Sensor Networks (WSN). *Journal of Information Processing Systems*, 6(2), 177-184.
13. Burgner D. E. & Wahsheh L. A. (2011). Security of Wireless Sensor Networks. Eighth International Conference on Information Technology: New Generations (ITNG), Las Vegas, NV, 315-320.
14. Perrig A., Stankovic J. & Wagner D. (2004). Security in Wireless Sensor Networks. *Communications of the ACM*, 47(6), 53–57.
15. Shim K. (2015). A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks. *IEEE Communications Surveys & Tutorials*, 18(1), 577-601.
16. Bysani L. K. & Turuk A. K. (2011). A Survey on Selective Forwarding Attack in Wireless Sensor Networks. IEEE International Conference on Devices and Communications (ICDCom), 1-5.
17. Kulkarni G., Shelk R., Gaikwad K., Solanke V., Gujar S. & Khatawkar P. (2013). Wireless sensor network security threats. Fifth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2013), Bangalore, 131-135.

18. Grover J., Sharma S. & Sharma M. (2014). Location Based Protocols in Wireless Sensor Network – A Review", IEEE Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT 2014), July 11-13, 2014, Hefei, Anhui, China, DOI: 10.1109/ICCCNT.2014.6962990, 1-5.
19. Manju. V. C (2012). A Survey on Wireless Sensor Network Attacks. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(2), 23-28.
20. Sharma K. & Ghose M. K. (2010). Wireless Sensor Networks: An Overview on its Security Threats. *IJCA Special Issue on Mobile Ad-hoc Networks (MANETs)*, 1(8), 42-45.
21. Nachabe L., Girod-Genet M. & El Hassan B. (2015). Unified Data Model for Wireless Sensor Network. *IEEE Sensors Journal*, 15(7), 3657-3667.
22. Grover J., Sharma S. & Sharma M. (2014). Reliable SPIN in Wireless Sensor Network. IEEE 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO 2014), October 8-10, 2014, Amity University, Noida, DOI: 10.1109/ICRITO.2014.7014694, 01-06.
23. Arora B. (2013). A Threat Model Approach for Classification of Network Layer Attacks in WSN. *International Journal of Computer Applications*, 63(9).
24. Akyildiz I., Su W., Sankarasubramaniam Y. & Cayirci E. (2002). A survey on sensor networks. *IEEE Communication Magazine*, 40(8), 102-114.
25. Jangra B. S. & Kumawat V. (2012). A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(3), 291-296.