Security in Wireless Sensor Network: A Survey

Tripti Sharma
Department Of Information Technology, Maharaja Surajmal Institute Of Technology, New Delhi,India-110058
triptionline@yahoo.com

Vaibhav Navani
Department Of Information Technology, Maharaja Surajmal Institute Of Technology, New Delhi,India-110058
vaibhavnavani1995@gmail.com

Abstract-Wireless Sensor Network (WSN) is gaining importance in modern application. WSNs are used to gather information in the form of images, signals, audios etc. remotely. The gathered information is sent to the receivers using special transducers. They are beneficial in many fields such as military purposes, wind speed calculation, for sensing forest fires etc. The main components of WSN are aggregation and Base System. Aggregation gathers data from the nearby environment, filters it and sends it to the Base System. However WSN are often limited in terms of memory and power and thus making it vulnerable to various security threats. In this paper, we focus on various WSN constraints and kinds of threat WSN faces.

Keywords- WSN, Security, Attacks**.**

I. Introduction

Wireless Sensor Network is an emerging technology whose task is to monitor and record conditions of the surrounding using aggregation and send it to the base system. They are low power low cost devices which are used to gather information of the surroundings and send it to the base system. These nodes are capable of sensing temperature, speed, humidity, pressure, movements of vehicles, noise levels, lighting conditions etc . Compact size, Cost effective, Memory storage for saving current data, Densely Deployed, Each node can gather data within a radius only are the characteristics of Wireless Sensor Nodes[1]. According to the types of need, WSN can be of four types. Terrestrial WSN, Underground WSN, Multimedia WSN, Underwater WSNare various types of wireless sensor network

Although WSNs are gaining importance, the security field is yet to achieve extensive focus. Factors like low power, low memory, bandwidth problems often pose great challenge to the developers and manufacturers because of small size and low cost[2]. Limitations of WSNs are as follows :- Low power, Low memory space, bandwidth problems, unreliable communication. Some of the measures have been taken to overcome these limitations but these efforts have not been fully successful like nodes which are placed at ground level are often equipped with solar cells to extend their battery life or using cryptographic keys to protect their data, sing Message identification code (MAC), monitoring or error correcting code. All the attacking techniques have different impact on the network and thus require different countering technique. The rest of the paper has been discussed as follows: - In Section 2, the importance of security in WSN has been discussed. In Section 3, various attacks and their possible solutions have been discussed on the basis of layer of network on which this attack occurs. Section 4 shows the comparisons of various attacks and their possible solutions on the basis of layer on which it attacks.

DOI- 10.18486/ijcsnt.2015.4.2.04
ISSN-2053-6283

Section 5 concludes the paper by giving brief summary.

II. Why Is There A Need For Security

Security ensures that no information is leaked or modified by any external source. Some of the reasons are stated below

A. TO ENSURE DATA CONFIDENTIALITY: - It is property in which only authorized users are given access to sensitive information. WSNs must ensure that the data is only to available to the certified group[3]. Sometimes due to larger distances, the data is sent through several nodes rather than a single node which makes it more vulnerable to attacks and thus requires better security. To ensure confidentiality, the data is often encrypted and only the certified users have the key to decrypt it.

B. TO ENSURE DATA INTEGRITY :- Data Integrity ensures that the data received has not been tampered with, that is, the data received by the trusted authority is the original message[3]. Some of the methods which ensure data are Watermarking Algorithm and Message Authentication Code(MAC). These methods prevent malicious users from meddling with the data.

C. TO ENSURE DATA AUTHENTICATION:- Data authenticity guarantees that the message received from the source is the trusted source. Authentication certifies that information about location, environment originates from the correct source [4].

D. TO ENSURE DATA FRESHNESS:- Confidentiality and authenticity are not enough, Data Freshness must also be taken into account. Data Freshness implies that the data transmitted by the sensors is recent and no old information is redirected again. Data Freshness is of two types : Weak and Strong. Weak freshness gives no information on delays, while strong freshness records such information[5]. Weak freshness is required for sensor measurements and strong freshness find its application in time synchronization.

E. TIME SYNCHRONIZATION:- Time Synchronization is used to economize the usage power by constantly switching off the power at times when not in use to prolong it's span. to power off at appropriate times some type time synchronization is required.

F. AVAILABILITY: - It ensures that the desired sensor network's services are still available at the time of attacks like denial of services. For making data available, sensors must utilize power and storage which can be accomplished by reusing code and following security protocols. Central node networks (star topology) should also be avoided as failure of head node can result in breakdown of whole network.

SECRECY :- Sensors are replaced frequently due to their short life span. It should be ensured that these nodes are not able to read any messages transmitted earlier or after it leaves it's work.

III. Types of Attacks

In this section, we are going to discuss on several attacks on the basis of layers of network .The attacks on the network can be of on directly or indirectly on the nodes in the network as shown in the fig 1.

1. Physical Layer:- It provides hardware means of sending and receiving data on some kind of carrier which can be data cables or any wireless medium. It is the only the layer which works on physical components.

Attacks on physical layer are as follows :

1.1 Jamming:- In jamming, the attackers interferes with the radio frequency which the network is using. This type of attack generally focuses on injecting false data which affects the data transmission and also reduce the efficiency of the network by draining the power of the nodes. There are many methods developed to detect and counter jamming attacks, some of which are carrier sensing time, packet delivery ratio, frequency hopping spread spectrum, code spreading etc.

DOI- 10.18486/ijcsnt.2015.4.2.04
ISSN-2053-6283

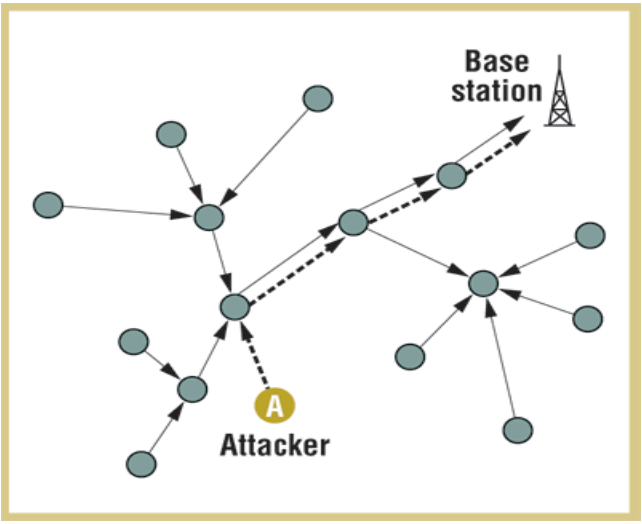

Figure 1. Example of attacker targeting a node.

1.2 Tampering :- Tampering is the process in which the attacker gets the access of the node. By gaining access, the attacker can retrieve sensitive information and also replace the node by his node which can be controlled by the attacker.

2. Link Layer :- In this layer, data is encoded and decoded into bits. It handles the errors faced in physical layer, flow control and frame synchronization. It is generally divided into Media Access Control(MAC) and Logical Link Control(LLC) layer. MAC controls how a computer access the data and permission to transmit the data[6] The LLC layer handles frame synchronization and error checking.

Attacks on link layer are as follows :

2.1. Collisions :- Collisions occur when two or more nodes try to transmit the data simultaneously. The

resultant package causes a mismatch at the receiving end

thus making the data received as invalid. A possible defense mechanism is error correcting code. However, they are only able to work in case of small collisions. But it is safe to assume that the attackers probably corrupts the data so much that it cannot be corrected.

2.2. Exhaustion :- Exhaustions occur when the nodes keeps on sending the despite several collisions. This attack results in over-utilization of the resources. Attackers use this method while attacking weak sensor networks which are naïve enough to send the data continuously unless stopped the user itself.One method to prevent exhaustion is by applying rate limit to MAC admission control [7]. Using this mechanism, if the nodes fail to transmit the data it can only try to retransmit it for specified number of times. Another solution to exhaustion is time division multiplexing.

3. Network Layer :- This layer provides switching and routing mechanisms to transmit the data from one place to another. This layer's job generally includes routing, addressing, internetworking, error handling and packet sequencing. In this layer power efficiency is an important requirement. Sensor networks are data centric.

3.1. Selective Forwarding :- Users generally assume that the nodes transmit all the messages it receives. Malicious attackers can attack a node and can make it send some information while drop other. One such attack is called Black Hole Attack where the node deletes all the information it receives thus disrupting the network. One way to prevent is by transmitting the data through multiple paths so even if one node is attacked the data is compromised. Another way to counter this information is by identifying the compromised node.

3.2 Sinkhole Attack :- It is an advanced form of Black hole attack where the attacker makes the compromised node look more friendly to the surrounding node so that the sensor nodes selects it as the next node for routing. This makes all the data from the nearby nodes to pass through it and thus placing the data in the hands of the attacker.

3.3 Sybil Attack :- It is a case in which one node identifies itself as several identities. It disrupts other fault tolerant schemes like network topology maintenance, fair resource allocation, data aggregation. The fake node occurs at several places at

DOI- 10.18486/ijcsnt.2015.4.2.04
ISSN-2053-6283

the same time and thus destroying the geographical protocols.

3.4 Wormholes :- A wormhole attack is a kind of attack which does not require cryptographic keys to attack therefore making it more difficult to detect. It usually occurs between two nodes. One end transmits the data via wormhole link and other end on receiving the data replays them to the local area and creating fake scenario that the node is only one or two step away from the location. Packet leashes is an effective way detect and counter wormhole attacks. They are generally of two types : geographical leash and temporal leash.

3.5 Hello Flood Attack :- In this type of attack, the malicious users send HELLO messages to the nodes with high radio transmission range using fake nodes. This creates an illusion that the fake nodes are neighbor nodes and thus the data transmits thorough this causing data congestion [5]. As the fake nodes generally creates an illusion of being the shortest route to the base station, all the data passes through it.

3.6 Acknowledgement Spoofing: - Sensor networks usually requires acknowledgements to be used in routing. The malicious node might spoof the acknowledgement in order to provide fake information to the neighboring nodes. One such false information includes that the current node provides the shortest path to the base station and therefore bleeding resources.

4. Transport Layer :- This layer is responsible for providing means to transfer information. It is responsible for managing end to end connections. It is also responsible for flow control and end to end error recovery.

4.1 De-synchronization :- In this type attack, the attacker tries to disrupt the whole network by constantly spoofing messages to the end node thus causing the node to waste energy by attempting to recover from the errors which ceases to exist.

4.2 Flooding :- In flooding, the adversary constantly requests for establishing connections to the selected node. With each request, some part of the resources are allocated to the adversary thus draining power and consuming memory.

5. Application Layer :- Application layer provides services for an application program to ensure that effective communication with another application program in a network is possible. It is not an application itself but a service layer.

5.1 Node- Replication Attack :- Every node has a unique ID. This ID is used to distinguish one node from another within a network[8]. The attacker might duplicate this ID and assign it to the attacking node. Since this node is recognized by the network, it can modify or drop or delete the data.

IV. Comparison Of Various Attacks On The Basis Of Network Layer And Their Possible Solutions

Comparison of various attacks on the basis of Network Layer and their possible solutions are given below in table 1.

Table 1: Comparison of various attacks

S. No	Type Of Attack	Layer On Which Attack Occurs	Possible Solution
1	Jamming	Physical	Code Spreading, Frequency Hopping Spread Spectrum
2	Tampering	Physical	Tamper proofing the physical nodes
3	Collision	Link	Error Correcting Code
4	Exhaustion	Link	Applying rate limit to MAC admission control
5	Selective Forwarding	Network	Multiple Path Usage, Identifying defected node
6	Sinkhole	Network	Authentication monitoring, redundancy
7	Sybil Attack	Network	Authentication
8	Wormhole	Network	Packet Leashes, Flexible Routing

DOI- 10.18486/ijcsnt.2015.4.2.04
ISSN-2053-6283

9	Hello Flood Attacks	Network	Two Way Authentication, Three way handshake
10	Flooding	Transport	Limiting Connection numbers, Client puzzles
11	Clone Attacking	Applicati on	Unique Pair-Wise Keys

IV. Conclusion

In this paper, the properties, types and limitations of the Wireless Sensor Networks have been discussed. This paper also provides detailed description of the attacks on sensor networks on the basis of network layers with their possible solution and the comparison has been made between the attacks on the basis of layer on which the attack occurs and the solutions to counter these attacks. Further it has been seen that different types of attacks have different possible solution.

References

[1] Zhenwei Yu, Jeffrey J.P. Tsai, A Framework of MachineLearning Based Intrusion Detection for Wireless Sensor Networks, IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing,2008.

[2] M. Yasir Malik, "An Outline of Security In Wireless Sensor Networks: Threats, Countermeasures and Implementations", Wireless Sensor and Energy Efficiency: Protocols, Routing and Management DOI: 10.4018/978-1-4666-0101 7.ch024

[3] X. Du, and H-H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications, vol. 15,no. 4, Aug. 2008, pp.60-66.

[4] Mona Sharifnejad, Mohsen Sharifi ,Mansoureh Ghiasabadi, Sareh Beheshti, "A Survey on Wireless Sensor Networks Security", SETIT 2007, 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, March 25-29, 2007 – TUNISIA.

[5] Singh, S.K., M. Singh and D. Singhtise, 2011." A survey on network security and attack defense mechanism for wireless sensor networks", International Journal of Computer Trends Tech, pp: 5-6.

[6] R.Venkatesha Prasad, P. Pawtczak, J. A Hoffmeyer,andH.S.Berger,"Cognitive functionality in next generation wireless networks: Standardization efforts," IEEE Communication Magazine, Vol. 46, Issue 4, pp. 72-78, April 2008.

[7] Orihashi, M., Nakagawa, Y., Murakami, Y., and Kobayashi, K., "Channel synthesized modulationemploying singular vector for secured access on physical layer", IEEE GLOBECOM 2003,Volume 3,1-5 December, 2003, pp. 1226 – 1230.

[8] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[9] G.S. Tomar and Shekhar Verma, "Dynamic multi-level hierarchal clustering approach for wireless sensor networks", International Journal of Simulation-Systems, Science and Technology, Vol.10, No. 4, pp 1-7, May 2009.

[10] M. Rai, Shekhar Verma, G.S. Tomar & Nittin Garg, "Local Repair for Extending Lifetime of Wireless Sensor Networks", International Journal of Computers & Electrical engineering, Vol.1, No.2, pp 191-198, Jun 2009.