ISSN: 2454-4248
317 – 322

A Review on Security Issues and Attacks in Wireless Sensor Networks

Dinesh Wasnik

Department of Computer Science and Engineering,

A.G.P.C.E., Nagpur.

Abstract**--** Wireless Sensor networks consists of hundreds or thousands of low cost, low power and self-organizing nodes which are highly distributed. Due to the reason that the sensor nodes are highly distributed, there is a need of security in the network. Security is an important issue nowadays in almost every network. There are some security issues and many attacks that need to be look around and work upon. This paper discusses some of the issues and the denial of service attacks of security.

Keywords*—Wireless sensor Networks, Types of WSN, Security, Security Concerns, Attacks.*

*****

I. Introduction

Wireless Sensor Networks are heterogeneous systems containing many small devices called sensor nodes and actuators with general-purpose computing elements. These networks will consist of hundreds or thousands of low cost, low power and self-organizing nodes which are highly distributed either inside the system or very close to it. These nodes consist of three main components-sensing, data processing and communication. Two other components are also there called, aggregation and base station [1]. Aggregation point's gathers data from their neighbouring nodes, integrates the collected data and then forwards it to the base station for further processing. Various applications of WSN includes habitat monitoring, manufacturing and logistics, environmental observation and forecast systems, military applications, health, home and office application and a variety of intelligent and smart systems.

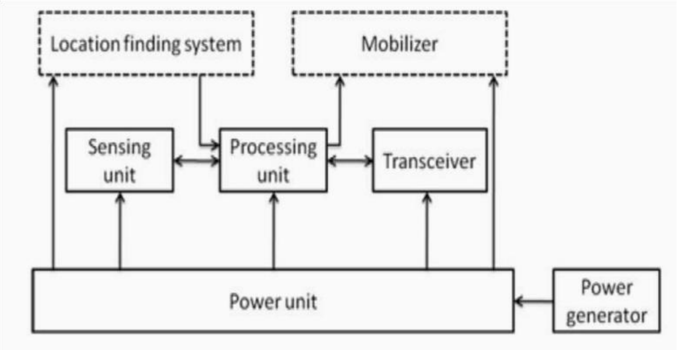

Fig. 1 Sensor node components

A.Characteristics of WSN[2]

1. Compact size
2. Physical security
3. Power
4. Memory space
5. Bandwidth
6. Unreliable communications

II. Types Of Sensor Networks

A.*Terrestrial WSNs[3]*

In these, nodes are distributed in a given area either in an ad hoc manner (sensor nodes are randomly placed into the target area by dropping it from plane) or in pre-planned manner (sensor nodes are placed according to grid placement, optimal placement, 2-d and 3-d placement models). Since battery power is limited and it cannot be recharged, terrestrial sensor nodes must be provided with an optional power source such as solar cells. B.*Underground WSNs[4]*

In these, sensor nodes are buried underground or in a cave or mine that monitors the underground conditions. Sink nodes are deployed above the ground to forward the gathered information from the sensor nodes to the base station. These are more expensive than the terrestrial sensor networks because proper nodes are to be selected that can assure reliable communication through soil, rock, water and other mineral contents.

C. *Underwater WSNs[4]*

In these, sensor nodes and vehicles are located underwater. Autonomous vehicles are used for gathering the data from the sensor nodes. Sparse deployment of nodes is done in this network. Main problems that come under this while communicating are limited bandwidth, long propagation delay and signal fading issue.

D. *Multimedia WSNs[5]*

In these, low cost sensor nodes are equipped with cameras and microphones. These nodes are located in a preplanned manner to guarantee coverage. Issues in these networks are demand of high bandwidth, high energy consumption, quality of service provisioning, data processing and compression techniques, and cross layer design.

III. Security in WSN

Security is one of the major aspects of any system. Traditional WSNs are affected by various types of attacks. These attacks can be categorized as:

1. Attacks on secrecy and authentication
2. Silent attacks on service integrity
3. Attacks on network availability

Cryptographic techniques can be used to prevent against the secrecy and authentication attacks. In silent attacks, the attacker compromises a sensor node and feeds wrong data. Attacks on network availability are also known as denial of service (DoS) attacks. If DoS attacks are promoted successfully, it can badly degrade the functioning of WSNs. Below we discuss the DoS attacks on different layers of networks [6].

A. *DoS attacks on the physical layer*

Physical layer is engaged with frequency selection, carrier frequency generation, signal detection, modulation and data encryption. Jamming is the most common way of injecting DoS attack on this layer.

B. *DoS attacks on the link layer*

Link layer is exposed to multiplexing of data streams, data frame detection, medium access control and error control. The attacks when elevated on this layer results in collision, resource exhaustion and unfairness in allocation of frames.

C. *DoS attacks on the network layer*

Network layer is exposed to different types of attacks such as spoofed routing information, selective forwarding, sinkhole, Sybil, wormhole, hello flood and acknowledgment flooding.

D. *DoS attacks on the transport layer*

Transport layer is exposed to flooding attack and de-synchronization attack.

E. *DoS attacks on the application layer*

Application layer is exposed to logic errors and buffer overflow.

IV. Security Concern InWsn

A. *Data Confidentiality*

Confidentiality is an acceptance of authorized access to information communicated from a certified sender to a certified receiver. A sensor network must not reveal sensor readings to its neighbours. Highly sensitive data is sometimes routed through many nodes before reaching the final node. For secure communication, encryption is used. Data is encrypted with a secret key that only authorized users have [7]. Public sensor information should also be encrypted to some degree to protect against traffic analysis attacks.

B. *Data Integrity*

Provision of data confidentiality stops the outflow of information [2], but it is not helpful against adding of data in the original message by attacker. Integrity of data needs to be assured in sensor networks, which strengthens that the received data has not been tampered with and that new data has not been added to the original contents of the packet. Data integrity can be provided by Message Authentication Code (MAC).

C. *Data Authentication*

An adversary is not only limited to modify the data packet but it can change the complete packet stream by adding extra packets. So the receiver needs to confirm that the data used in any decision-making process comes from the authorized source [8]. Data authenticity is an assurance of the identities of communicating nodes.

Nodes taking part in the communication must be capable of recognizing and rejecting the information from illegal nodes. Authentication is required for many administrative tasks.

D. *Data Freshness*

Data freshness ensures that the data communicated is recent and no previous messages have been replayed by an adversary. Data freshness is classified into two types based on the message ordering [9]; weak and strong freshness. Weak freshness provides only partial message ordering but gives no information related to the delay and latency of the message. Strong freshness on the other hand, gives complete request-response pair and allows the delay estimation. Sensor measurements require weak freshness, while strong freshness is needed for time synchronization within the network. For ensuring the freshness of a packet, a timestamp can be attached to it. Destination node can compare the timestamp with its own time clock and checks whether the packet is valid or not.

E. *Availability*

Availability is an insurance of the endowment to indulge expected services as they are designed earlier. It guarantees that the network services are feasible even in the subsistence of denial of service attacks. For making data available, security protocol should obsess less energy and storage, which can be targeted by the reuse of code and making sure that there is slight increase in communication due to the functioning of security protocols. Central point scheme should also be avoided as single point failure will be introduced due to this in a network that threatens the availability [8].

F. *Self Organization*

A typical WSN may have thousands of nodes fulfilling various operations, installed at different locations. Sensor networks are also ad hoc networks, having the same flexibility and extensibility. Sensor networks crave every sensor node to be independent and ductile enough to be self-organizing and self-healing according to different situations [8].

G. *Time Synchronization*

Most sensor network applications depend upon some form of time synchronization. In order to skimp power, an individual sensor’s radio may be turned off for some time. Moreover, sensors may wish to calculate the end-toend delay of a packet as it travels between two pair wise sensors [10].

H. *Secure Localization*

WSN makes use of geological based information for recognition of nodes, or for accessing whether the sensors correspond to the network or not. Some attacks work by investigating the location of the nodes. Attacker may probe the headers of the packets and protocol layer data for this purpose. This makes the secure localization an important feature that must be satisfied during our implementation of security protocol [2].

I. *Flexibility*

Sensor networks will be used in vigorous arena scenarios where environmental circumstances, hazards and mission may change frequently. Changing mission goals may desire sensors to be eliminated from or injected to a settled sensor node. Moreover, two or more sensor networks may be merged into one, or a single network may be divided in two. Key establishment protocols must be ductile enough to render keying for all potential scenarios a sensor network may encounter [11].

J. *Robustness and Survivability*

The sensor network should be robust across various security attacks and if an attack conquers, its impact should be reduced. The covenant of a single node must not violate the security of the whole network [9].

V. Attacks

Wireless sensor networks are power constraint networks, having limited computational and energy resources. This makes them exposed enough to be attacked by any attacker deploying more resources than any individual node or base station, which may not be a difficult job for the attacker. A typical sensor network may be comprised of potentially hundreds of nodes which may use broadcast or multicast transmission. The broadcast nature of the transmission medium is the reason why wireless sensor networks are susceptible to security attacks. Denial of Service attack eradicates a network’s range to satisfy its expected function. Various DoS attacks on different layers are discussed below.

A. *Jamming*

Jamming is one of the basic yet destructive attacks that attempt to interrupt in physical layer of the WSN structure. Jamming can be of two types- constant jamming and intermittent jamming. Constant jamming affects the complete obstruct of the whole network whereas in intermittent jamming nodes are capable of communicating data periodically but not continuously.

B. *Physical Attacks*

Physical attacks give the adversary the endowment to reconstruct the nodes and thus the network functioning at physical layer. The attacker can abstract source code which ultimately provides attacker the information about the network that can alter the code to get admittance into the network. Attacker can substitute the nodes with the illegal and detrimental ones, thus negotiating the functioning of the whole sensor network. Various types of physical attacks are listed below in the table [1] with their definitions, threats and effects.

Attacks	Definition	Threat	Effects
Signal/ radio jamming	The attacker tries to transfer radio signals issued by the sensors to the receiving antenna.	Availability, integrity	Radio interference, resource exhaustion
Device tampering attack, node capturing attack	Direct physical approach, conquered and redeem nodes	Availability, integrity, authenticity, confidentiality	Corrupt/ transform physically, halt/modify node's functions, software susceptibilities, fully manages the hooked nodes
Path-Based DOS	Amalgamation of attacks	Availability, authenticity	Nodes battery discharge, network interruption, minimizing network's availability
Node outage	Halting the working of nodes	Availability, integrity	Halts nodes operations, bombarding a diversity of other attacks
Eavesdropping	Observing the essence of conversation by tapping venture to information	Confidentiality	Bombarding other attacks, citing delicate data, remove the privacy protection and minimizing data confidentiality

C. *Collision*

Collision is a type of link layer jamming that occurs when two nodes try to transfer data at the same time and at the same frequency [14]. An attacker may cause collisions in particular packets such as ACK control messages. The effected packets are transmitted again, increasing the energy and time cost for transmission. Such an attack reduces the network perfection.

D. *Exhaustion*

Exhaustion occurs at the link layer. This attack dominates the power resources of the nodes by causing them to retransmit the message even when there is no collision or late collision [2].

E. *Unfairness*

MAC protocols at link layer administer the communications in networks by constraining priority schemes for seamless correlation. It is possible to use these protocols thus affecting the precedence schemes, which ultimately results in decrease in service [2].

F. *Neglect and Greed Attack*

This attack occurs at the network layer [6]. When a packet is transmitted from a sender to a receiver, then in between both these nodes, there occur a number of other nodes through which the packet is routed before reaching to the final destination. Transmission is said to be successful when the packet is completely reached to its destination. In the meanwhile, malicious node can force multi-hopping in the network, either by splashing some packets or by routing the packets towards a wrong node. This attack disturbs the behaviour of the adjoining nodes, which may not be able to receive or send messages.

G. *Homing*

In homing attack, the attacker investigates the network traffic at the network layer to interpret the geological area of cluster heads or base station adjoining nodes. It then implements some other attacks on these crucial nodes, so as to physically destroy them that further cause major destruction to the network [2].

H. *Routing Information Alteration (spoofing)*

It occurs at the network layer [6]. In this, an adversary spots the routing information in the network by modifying or replaying the routing information to disturb the traffic in the network. This attack can create new routing paths, attracts or repels the network traffic from selected nodes, lengthen or shorten the source routes, generates false error messages, causes network division and maximizes the end-to-end latency.

I. *Black holes*

Also known as sink holes occurring at the network layer [12]. It builds a covenant node that seems to be very attractive in the sense that it promotes zero-cost routes to neighbouring nodes with respect to the routing algorithm. This results maximum traffic to flow towards these fake nodes. Nodes adjoining to these harmful nodes collide for immense bandwidth, thus resulting into resource contention and message destruction.

J. *Flooding*

Flooding also occurs at the network layer [6]. An adversary constantly sends requests for connection establishment to the selected node. To hit each request, some resources are allocated to the adversary by the targeted node. This may result into effusion of the memory and energy resources of the node being bombarded.

K. *Sybil Attack*

This again is a network layer attack. In this, an awful node presents more than one character in a network. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks [10]. The Sybil attack is efficient enough to stroke other fault tolerant schemes such as dispersity, multi path routing, routing algorithms, data aggregation, voting, fair resource allocation, topology maintenance and misbehaviour detection. The fake node implies various identities to other nodes in the network and thus occurs to be in more than one place at a time. In this way, it disturbs the geographical routing protocols. It can collide the routing algorithms by constructing many routes from only one node.

L. *Selective Forwarding*

Selective forwarding is a network layer attack [13]. In this, an adversary covenants a node, that it scrupulously forwards some messages and plunge the others. This hampers the quality of service in WSN. If the attacker will drop all the packets then the adjoining nodes will become conscious and may evaluate it to be a flaw. To avoid this, the attacker smartly forwards the selective data. To figure out this type of attack is a very tedious job.

M. *Worm holes*

In the wormhole attack, pair of awful nodes firstly discovers a wormhole at the network layer [12]. A wormhole is a low-latency junction between two sections of a network. The malicious node receives packets in one section of the network and sends them to another section of the network. These packets are then replayed locally. This creates a fake scenario that the original sender is only one or two nodes away from the remote location. This may cause congestion and retransmission of packets squandering the energy of innocent nodes.

N. *Hello Flood Attacks*

Hello flood attack uses HELLO message to advertise itself to its adjoining nodes and a node receiving this message may consider that it is within radio vicinity of the sensor. In this type of attack, an adversary with a high radio transmission range and processing power sends HELLO message to a number of sensor nodes which are scattered in a large area within a WSN. It gives an illusion that the malicious node is their neighbour. When the assured nodes will send message to the base station, then it passes through the malicious node as this node provides the shortest route to the base station as an illusion. When the information reaches the attacker, the victim is betrayed by it. This leads to data congestion and thus complicates the data flow in the network [2, 10].

O. *Acknowledgement Spoofing*

Acknowledgements play a significant role in certifying the quality of service and creating another links. Acknowledgement spoofing attack is introduced on routing algorithms at the network layer that needs transmission of acknowledgement messages. An attacker may eavesdrop packet transference from its adjoining nodes and swindle the acknowledgements, thereby sending wrong information to the nodes [2].

P. *De-synchronization*

De-synchronization occurs at the transport layer [14]. This attack tries to disturb an existing connection. An adversary continuously swindles packets to an end host. This host then demands retransmission of dropped frames and hence the energy of nodes is wasted, therefore degrading the performance of the whole network.

Q. *Interrogation*

An interrogation attack imposes on the two way handshake (request-to-send/clear-to-send) that several MAC protocols use to reduce the hidden-node problem. An adversary can misuse a node’s resources by frequently sending RTS messages to obtain CTS responses from a directed adjoining node [2].

R. *Node Replication Attack*

Every sensor node in a network has a unique ID. This ID can be duplicated by an attacker and is assigned to a new added malicious node in the network. This assures that the node is in the network and it can lead to various calamitous effects to the sensor network. By using the replicated node, packets passing through malicious node can be missed, misrouted or modified. This results in wrong information of packet, loss of connection, data loss and high end-to-end latency. Malicious node can get authority to the sensitive information and thus can harm the network [2].

VI. CONCLUSION

In this paper, we present a brief survey on wireless sensor network, its characteristics and its types. Then we discussed about the security in sensor networks, security issues and various DoS attacks on different layers. Security is an important requirement and complicates enough to set up in different domains of WSN. We also discuss various dimensions of security (availability, integrity, confidentiality and authenticity) that are being directed by different physical attacks.

References

[1] Rina Bhattacharya, "A Comparative Study of Physical Attacks on Wireless Sensor Networks", *IJRET,* vol. 2, issue 1, pp. 72-74, Jan 2013

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

[3] I.F. Akyildiz, W. Su, Y.Sankarasubramaniam, E. Cayirci, "A survey on sensor networks", *IEEE Communications Magazine* 40 (8) (2002) 104–112

[4] I.F. Akyildiz, E.P. Stuntebeck, "Wireless underground sensor networks: research challenges", *Ad-Hoc Networks* 4 (2006) 669–686

[5] Kriti Jain, UpasanaBahuguna, "Survey on Wireless Sensor Network", *IJSTM,* Vol. 3 Issue 2, pp. 83-90, Sept 2012 [6] JaydipSen, *Security and Privacy Challenges in Cognitive Wireless Sensor Networks*, Dec 2012

[7] Shio Kumar Singh, M P Singh, D K Singh, "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks", *International Journal of Computer Trends and Technology-*, May to June Issue 2011, ISSN: 2231-2803

[8] Dr. Manoj Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges", *IJCIT*, vol. 2, issue 1, pp. 62-67, 2011

[9] SnehlataYadav, Kamlesh Gupta, Sanjay Silakari, "Security issues in wireless sensor networks", *Journal of Information Systems and Communication,* vol. 1, issue 2, 2010, pp-01-06

[10] Pooja , Manisha, Dr. Yudhvir Singh, "Security Issues and Sybil Attack in Wireless Sensor Networks", *InternationalJournal of P2P Network Trends and Technology,* vol. 3, issue 1, pp. 7-13, 2013

[11] Mona Sharifnejad, Mohsen Sharifi, MansourehGhiasabadi, SarehBeheshti, **"**A Survey on Wireless Sensor
Networks Security", SETIT 2007, *4th International Conference: **S**ciences of **E**lectronic, **T**echnologies of **I**nformation and **T**elecommunications,* March 25-29, 2007 – TUNISIA

[12] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In *Proc. of the 1st IEEE Int. Workshop on Sensor Network Protocols and Applications(SNPA'03)*, pp. 113-127, May 2003

[13] X. Wang, W. Gu, K. Schosek, S. Chellappan, D.Xuan, "Sensor network configuration under physical attacks", *International Journal of Ad Hoc and Ubiquitous Computing*, Vol 4, Issue 3/4, pp. 174-182, April 2009

[14] A.D. Wood, J.A. Stankovic, "Denial of service in sensor networks", *IEEE Computer*, Vol. 35, Issue 10, pp. 5462, October 2002