International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Review on Security Challenges and Attacks in Wireless Sensor Networks

Paramjit Kour[1], Lal Chand Panwar[2]

[1]M. Tech student, Punjabi University Patiala, India

[2]Assistant Professor (CE), Punjabi University Patiala, India

Abstract: ***Wireless Sensor Network is emerging technology with their limited energy, computation, and communication capabilities. In contrast to traditional networks, wireless sensor networks are set out in penetrable areas and interact closely with the physical environment, results in increasing the risk of physical attacks; because of these reasons current security mechanisms are inadequate in WSN. In order to facilitate applications that require packet delivery from one or multiple senders to one or multiple receivers must need appropriate security methods. In this paper, we present the review of attacks and security challenges in Wireless sensor networks. First we outline the security constraints, goals, and then attacks with their corresponding prevention and detection mechanisms. At the end we present a comprehensive view of security threats and the layers affected.***

Keywords*:* Security, Attacks, sensor, networks, DOS, WSN

1. Introduction

A WSN can be defined as a network of devices, denoted as sensor nodes, which can sense the environmental conditions such as temperature, sound, pressure etc. and communicate the information gathered from the monitored field (e.g. an area or volume) through wireless links [1]. The data is forwarded, possibly via multiple hops, to a sink (sometimes denoted as controller or monitor) that can use it locally or is connected to other networks (e.g., the Internet) through a gateway. The nodes can be stationary or moving. They can be aware of their location or not. They can be homogeneous or not. The main basic goals of wireless sensor network are to sense information from the surrounding environment and pass it through the network to main location. WSN have attracted much attention due to its great potential to be used in various applications such as battlefield surveillance, many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring etc. The foremost challenge for sensor networks consists of two facts. First, sensors are extremely resource constrained. Second, in many applications sensor nodes will be randomly deployed. This random deployment raises issue of dimensioning the network. Scattering too few nodes may result in lack of field coverage and disconnection in the network. On the other hand, scattering many nodes may result in an efficient network due to increased medium access control (MAC) collision and interference. Thus, because of the limited resources on sensor nodes, size and density of the networks, unknown topology prior to deployment, and high risk of physical attacks to unattended sensors, wireless sensor networks becomes vulnerable to various attacks.

2. Need of separate security mechanism for WSN

In spite of traditional networks, wireless sensor networks are deployed in accessible areas, presenting a risk of physical attacks; because of these reasons current security mechanisms are inadequate in WSN. As demand of wireless sensor network is increasing day by day, much advancement is also going on. If compare to traditional networks they are still suffering from challenges such as ad-hoc nature, wireless medium, storage space, routing, battery power. Thus we need some separate security mechanisms for WSN which are discussed below.

- Due to various limitations like memory, power, battery etc existing security mechanisms are poor fit for this domain.
- Threats to sensor networks are different from threats to mobile ad-hoc networks.
- Traffic model in WSN is many to in contrast to mobile ad-hoc models where it is many to many.
- Sensor nodes are vulnerable to failures due to harsh deployment environmental conditions.
- Number of nodes in WSN can be several orders of magnitude higher than the nodes in the ad-hoc network. Thus WSN needed more flexible security mechanism.
- Sensor nodes may not have global identification.
- Because of high mobility nature nodes network topology always gets change. Thus security mechanism should be educate enough to prevent attacks within dynamic network.
- As sensor nodes are tiny devices and for operation they need a continuous power supply which is little bit tough to provide every where all time. Failure of any sensor node may cause the failure of whole network. So it is also the point of concern.
- Many applications require synchronization among sensor nodes which is difficult to achieve due to different types of delays like node processing and multi-hop routing delays. Thus we need a effective security mechanism to achieve synchronization.

3. Security goals for sensor networks

The security goal for WSN is to provide confidentiality, integrity, authenticity and availability of all information in limited resource constraints. As the sensor networks can also

operate in an ad-hoc manner thus the security goals must covers the goals for traditional networks requirements as well as the unique requirements suited to the constraints of wireless sensor networks. The security goals are classified as primary and secondary [5]. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability. The secondary goals are Data Freshness, Self- Organization and forward and backward secrecy. The security goals are discussed in detail below.

3.1 Data Confidentiality

Data Confidentiality ensures that a given message cannot be understood by anyone other than the intended recipients. This is one of the important goal in the network security. A sensor node should not disclose its data to the neighbors. Confidentiality can be achieved through the use of various encryption schemes.

3.2 Data Integrity

Data integrity is to ensure that information is not changed in transit either due to malicious intent or by accident. Even if the network has confidentiality measure procedures, there is still a possibility that the data integrity has been compromised. Data integrity can be maintained by using various integrity constraints and Message Authentication Code (MAC).

3.3 Data Authentication

Authentication ensures the reliability of the message by identifying its origin. Data authentication validates the identity of the senders and receivers. Data authentication is ensured through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys. Due to the wireless and the unguarded nature of sensor networks, it is extremely challenging to achieve authentication.

3.4 Data Availability

Data availability determines whether a node has the ability to use the resources and whether the network is available for the nodes to communicate. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network. The requirement of proper security mechanism not only affects the operation of the network, but also is highly important in maintaining the availability of the network.

3.5 Data Freshness

Even if confidentiality and data integrity are ensured, there is a need to ensure the freshness of each message. Informally, data freshness [4] requires that the data is recent, and it ensures that no old messages have been sent. To solve this problem time related counter can be added into the packet and shared key mechanism can be changed time to time in order to achieve data freshness.

3.6 Self-Organization

A wireless sensor network is a typically an ad-hoc network, which requires every sensor node to be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no particular framework available for the purpose of network management in a sensor network. This inherent feature poses a great challenge to wireless sensor network security. If self organization is lacking in a sensor network, the damage resulting from an attack or even the risky environment may be harmful for the network.

3.7 Time Synchronization

Most sensor network applications based on some form of time synchronization. Furthermore, sensors may want o compute the end-to-end delay of a packet as it travels between two pair-wise sensors. A more collaborative sensor network may require group synchronization [4] for tracking applications.

3.8 Secure Localization

Often, the usefulness of a sensor network will based on its ability to accurately and automatically locates each sensor in the network. A sensor network designed to find faults because it needed accurate location information in order to locate the fault. Unfortunately, an attacker can easily alter non-secured location information by sending false signal strengths and replaying signals.

3.9 Forward and Backward secrecy

Forward secrecy ensures that a sensor should not be able to read any future messages after it leaves the network. Backward secrecy ensures that a joining sensor should not be able to read any previously transmitted message.

4. Type of Attacks on WSN

4.1 Jamming

Jamming is a type of DOS attack which interferes with the radio frequencies that a network's nodes are using [3, 5]. A jamming source may either be powerful enough to disrupt the entire network or less powerful and only be able to disrupt a smaller portion of the network.

Defense mechanism- Typical defenses against jamming involves the use of various spread-spectrum communication techniques such as frequency hopping and code spreading.

4.2 Tampering

Another physical layer attack is tampering [5]. Given physical access to a node, an adversary can extract sensitive information such as cryptographic keys or other data on the node. The node may also be altered or replaced to create a compromised node which is controlled by attacker.

Defense Mechanism - One defense to this attack involves tamper-proofing of nodes. However, it is usually assumed that the sensor nodes are not tamper-proofed in WSN due to the additional cost. This indicates that a security scheme must consider the situation in which sensor nodes are compromised.

4.3 Collisions

A collision occurs when two nodes attempt to transmit on the same frequency simultaneously [8]. When packets collide, a change will likely occur in the data portion, causing a checksum mismatch at the receiving end. The packet will then be discarded as invalid. An adversary may strategically cause collisions in specific packets such as ACK control messages. A possible result of such collisions is the costly exponential back-off in certain media access control (MAC) protocols.
Defense mechanism- A typical defense against collisions is the use of error-correcting codes [5].

4.4 Exhaustion

Repeated collisions can also be used by an attacker to cause resource exhaustion. For example, a naive link-layer implementation may continuously attempt to retransmit the corrupted packets. Unless these hopeless retransmissions are discovered or prevented, the energy reserves of the transmitting node and those surrounding it will be quickly depleted.
Defense mechanism- One possible solution is to apply rate limits to the MAC admission control such that the network can ignore excessive requests, thus preventing the energy drain caused by repeated transmissions. A second technique is to use time-division multiplexing where each node is allotted a time slot in which it can transmit [10].

4.5 Unfairness

Unfairness can be considered a weak form of a DoS attack [5]. An attacker may cause unfairness in a network by intermittently using the above link-layer attacks. Instead of preventing access to a service outright, an attacker can degrade it in order to gain an advantage such as causing other nodes in a real-time MAC protocol to miss their transmission deadline. **Defence mechanism-** One defence mechanism is the use of small frames which lessens the effect of such attacks by reducing the amount of time an attacker can capture the communication channel. However, this technique often reduces efficiency and is susceptible to further unfairness.

4.6 Selective Forwarding

A significant assumption made in multihop networks is that all nodes in the network will accurately forward received messages. An attacker may create malicious nodes which selectively forward only certain messages and simply drop others [10]. A specific form of this attack is the black hole attack in which a node drops all messages it receives.

Defence mechanism- One defence against selective forwarding attacks is using multiple paths to send data [10]. A second defence is to detect the malicious node or assume it has failed and seek an alternative route.

4.7 Sinkhole

In a sinkhole attack, an attacker makes a compromised node look more attractive to surrounding nodes by forging routing information .The end result is that surrounding nodes will choose the compromised node as the next node to route their data through. This type of attack makes selective forwarding very simple, as all traffic from a large area in the network will flow through the adversary's node.

Defence mechanism- The defence mechanism against this type of attack is the use of hierarchical and dynamic routing.

4.8 Sybil attack

The Sybil attack is a case where one node poses more than one identity in the network [3]. Protocols and algorithms which are easily affected include fault-tolerant schemes, distributed storage, and network-topology maintenance. For example, a distributed storage scheme may rely on there being three replicas of the same data to achieve a given level of redundancy. If a compromised node pretends to be two of the three nodes, the algorithms used may conclude that redundancy has been achieved while in reality it has not.

Defense mechanism- The type of attack can be prevented through the use of digital certificates and public key encryptions.

4.9 Wormholes

A wormhole is a low-latency link between two portions of the network over which an attacker replays network messages [7]. This link may be established either by a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or by a pair of nodes in different parts of the network communicating with each other. The latter case is closely related to the sinkhole attack, as an attacking node near the base station can provide a one-hop link to that base station via the other attacking node in a distant part of the network.

Defense mechanism- A novel and general mechanism packet leaches can be used for detecting and defending against wormhole attacks.

4.10 Hello Flood Attacks

Many protocols which use HELLO packets make the naive assumption that receiving such a packet means the sender is within radio range and is therefore a neighbor. An attacker may use a high-powered transmitter to trick a large area of nodes into believing they are neighbors of that transmitting node [11]. If the attacker falsely broadcasts a superior route to the base station, all of these nodes will attempt transmission to the attacking node, despite many being out of radio range in reality.

Defense mechanism- These types of attacks can be prevented through the use of authenticated broadcast protocols.

4.11 Acknowledgment Spoofing

Routing algorithms used in sensor networks sometimes require Acknowledgments to be used. An attacking node can spoof the Acknowledgments of overheard packets destined for neighboring nodes in order to provide false information to those neighboring nodes [9]. An example of such false information is claiming that a node is alive when in fact it is dead.

4.12 Black Hole Attack

The black hole attack [1] position a node in range of the sink and attracts the entire traffic to be routed through it by advertising itself as the shortest route. The attacker drops packets coming from specific sources in the network. This attack can isolate certain nodes from the base station and creates a discontinuity in network connectivity.

Defense mechanism- This type of attack can be by using appropriate prevention and detection algorithms like by setting up a threshold old value for transmission range of each node.

4.13 Node Replication Attack

This is an attack where attacker tries to mount several nodes with same identity at different places of existing network. There two methods for mounting this attack. In first method the attacker captures one node from the network and creates clone of a captured node and mounts in different places of the network. In second method attacker may generate a false identification of a node then makes clone nodes tries to generate false data to disrupt the network. Node replication attack is different form Sybil attack. In Sybil attack a single node exists with multiple identities but in node replication attack multiple nodes present with same identity.

Defense mechanism- This type of attack can be detected by using various centralized and distributed detection techniques.

4.14 De-synchronization

De-synchronization refers to the disruption of an existing connection [2]. An attacker may, for example, repeatedly spoof messages to an end host, causing that host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data, thus causing them to instead waste energy by attempting to recover from errors which never really existed.

Defense mechanism- A possible solution to this type of attack is to require authentication of all packets communicated between hosts [5].

5. Conclusion

In this paper, we present a review on security challenges and attacks in wireless sensor networks. Then we discussed about the need for separate security mechanism and various dimensions of security (availability, integrity, confidentiality and authenticity) that are being directed by different physical attacks. This also includes the definitions of attacks and their defense mechanisms. This survey will hopefully motivate future researchers to come up with smarter and more robust security mechanisms and make their network safer. In table 1 various security schemes are summarized for wireless sensor network.

Table 1: Summary of Attacks in Wireless Sensor Network

Attacks	*Layer Affected*	*Security Threats*
Jamming, Tampering	Physical	Availability, Integrity
Collisions, Exhaustion, Unfairness	Data Link layer	Confidentiality, Integrity,
Spoofing, Selective Forwarding, Sybil, sinkhole, Wormhole, Node Replication	Network Layer	Availability, Authentication, Confidentiality
Flooding, De-synchronization	Transport Layer	Availability

References

[1] Zoran S.Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, “Security Issues in Wireless Sensor Networks”, International Journal of Communication, Issue 1, Volume 2, 2008
[2] Sachin Umrao, Arun Kumar, Praveet Umrao "Security Attacks and their Countermeasures along with Node Replication Attack for Time Synchronization in Wireless Sensor Network” International Conference on Advanced Nano-materials & Emerging Engineering Technologies, 24 to26 July, 2013, pp-576-581.
[3] Asmae BLILAT, Anas BOUAYAD, Nour el houda CHAOUI, Mohammed EL GHAZI (2012), “Wireless Sensor Network: Security challenges”, 978-1-4673-1053-6/12/2012 IEEE.
[4] Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala “Security in Wireless Sensor Networks: Issues and Challenges” IEEE International Conference on Space Science and Communication (Icon Space), 1-3 July 2013, pp-356-360.
[5] Kai Xing, Shyaam Sundhar, Manny Rivera, Xiuzhen Cheng “Network Security”, Springer, New York, 2005.
[6] S. K. Singh, M. P. Singh, and 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.
[7] Ms.Kshitija A.Chaple, “Taxonomy For Wsn Security” International Journal of Computers & Technology Volume 4 No. 2, March-April, 2013 pp- 295-308.
[8] Aashima Singla, Ratika Sachdeva, “Review on Security Issues and Attacks in Wireless Sensor Networks,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, April 2013, pp. 529–534.

[9] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4 No.2009.
[10] Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats," IJCA Special Issue on "Mobile Ad-hoc Network -February 2010.