



Analysis of Security Attacks in Wireless Sensor Networks

Divya Singla¹, Chander Diwaker²

¹CSE Department

²Assistant Professor CSE Department

U.I.E.T. Kurukshetra University

Kurukshetra University, Haryana, India

Abstract: A Wireless Sensor Network is a collection of thousands of sensor nodes which are distributed in a wireless and infrastructure-less environment to carry out some sensing application. These networks are useful in several applications like fire-fighting, military applications, area monitoring etc. This paper addresses the security issues, goals and attacks on WSN because Wireless Sensor Networks are more vulnerable. Several techniques are being developed by the many researchers to handle attacks are discussed.

Keywords: Wireless Sensor Networks (WSN); MANET; Sensor nodes; Attacks; Security issues.

I. Introduction

Wireless Sensor Network is a distributed network of sensor nodes deployed in wireless medium to measure temperature, pressure, sound, motion etc. WSNs form an ad-hoc network that operates with nominal or no infrastructure. Some of the characteristics of WSN are: ability to cope up with node failures, ability to tackle harsh environmental conditions, having dynamic network topology. The sensor nodes in WSN are resource constrained which define its limitations of processing capability, storage capacity, communication bandwidth and energy. There are two types of wireless networks-MANET and WSN. MANET poses to be an excellent choice where the construction and destruction of networks take place on adhocism. Both the networks differ in terms of addressing, scalability, active networking and energy.

II. Applications

WSN has many varied applications. Some of the applications strictly used in WSN are as follows:

- Nuclear reactor control
- Traffic monitoring
- Seismic Monitoring
- Environmental monitoring
- Fire detection
- Contaminant Transport

III. Security Requirements

The major concern in WSN is to give security services such as authentication, confidentiality, integrity, availability etc. It is very essential to save WSNs from malevolent attacks in unfriendly situations. Such networks require security plan due to various limitations of resources and the prominent characteristics of a wireless sensor network which is a considerable challenge. Security issues come from the attacks and threats. WSN are being used in the military like battlefields. So, it is necessary to design security mechanisms according to the requirements because it is the special feature of setting up WSN. The Wireless Technology acquires various security threats and there are varieties of securities available to prevent security attacks.

IV. Security Issues

When dealing with security in WSNs, we mainly focus on the problem of achieving some of all of the following security contributes or services. There are various security issues in WSN as follows:[3]

- **Confidentiality:** Confidentiality ensures that certain information is only readable or accessible by the authorized nodes.
- **Integrity:** It guarantees that the authorized parties are only allowed to modify the information or data and ensures that data during transmission is not altered or tempered.
- **Authentication:** It ensures that the retrieval and sending of data is done by the authorized parties by identifying its origin.
- **Availability:** Availability ensures that the network is available even in the presence of denial-of-service attacks. However failure of central hub or cluster head may make a node unavailable for use.

- **Freshness:** Freshness ensures that the data is recent and old messages are not replayed. Even though Integrity and confidentiality is there, data freshness is to be checked separately.

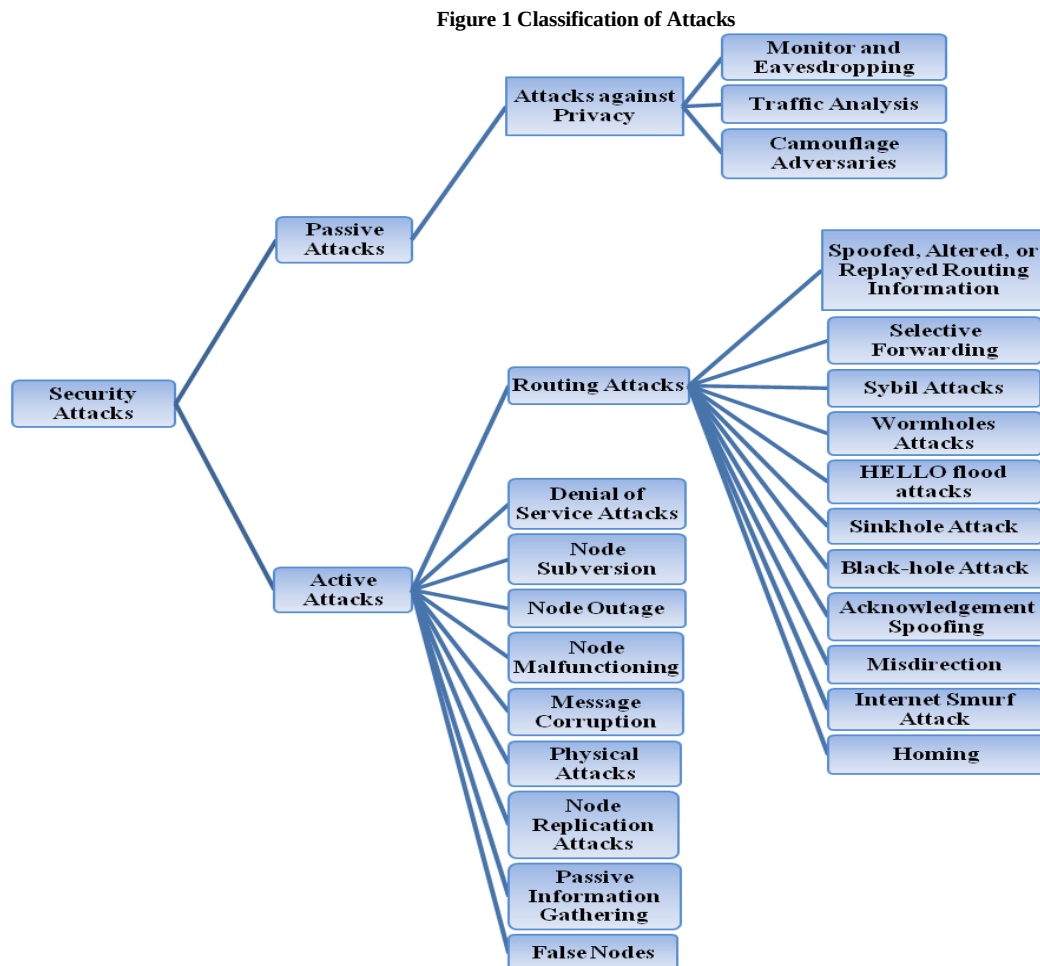
V. Security Challenges

Designing a threats free security protocols for wireless networks is a very challenging task. It represents significant challenges in designing security schemes. [2]

- Wireless medium is the challenging factor because it is less secure.
- Mobility of nodes and its large scalability makes the network more complex.
- Bandwidth, memory, computational complexity, energy are the major concern for designing the security mechanisms.
- The transmission range of sensor nodes is very limited because of saving energy.
- WSN nodes are placed in the hostile environment where they are not protected physically.
- To meet out such mixed traffic demands WSNs have to be scalable as needed by the applications.

VI. Attacks and Threats

Due to the wireless nature and infrastructure-less environment of WSN, they are more vulnerable to many types of security attacks. Security issues mainly come from attacks. If there is no attacks occurred then no need of security. Because of broadcast nature of communication always there is threat of attacks. Attackers may attack the WSN with different types of security threats to make the system unstable. Generally, there are two types of attacks: External attacks and Internal Attacks. In an external attack, the attacker node is not an authorized participant of the sensor network. This is further classified into Active and Passive attacks. The following diagram shows classification of attacks in sensor networks.



A. *Passive Attacks*

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. [5]

1. **Attacks against Privacy:** Passive attacks are also known as Attacks against Privacy. There are some common attacks against privacy are:
 - *Monitor and Eavesdropping:* By snooping to the data, the adversary could easily discover the communication contents.
 - *Traffic Analysis:* If the message which is transferred is encrypted then also there is risk of malicious harm.
 - *Camouflage Adversaries:* Intruder inserts their node or compromises the nodes to hide and then it can copy as a normal node to attract the packets.

B. *Active Attacks*

When the Intruders senses the data stream and alter the information during the transmission are known as active attacks. There are some attacks given below: [5]

1. **Routing attacks:** The attacks which acts on the network layer are called routing attacks. The following are the attacks that happen while routing the messages.
 - *Spoofed, Altered, or Replayed Routing Information:* In order to disturb traffic, an attacker may alter, spoof or replay routing information in the network.
 - *Selective Forwarding:* An attacker may create malicious nodes which selectively forward only certain messages and simply drop others.
 - *Sybil Attacks:* The Sybil Attacks targets the fault tolerant schemes like multipath routing, topology maintenance and distributed storage.
 - *Wormholes Attacks:* An attacker collect packets of data at one particular location in the network, transfers them to some other location, and then resend them into the network.
 - *HELLO flood attacks:* A malicious node sends or re-plays the routing protocol HELLO packets from one node to another with more power.
 - *Sinkhole Attack:* When the whole traffic is attracted at a specific node then it is called as sinkhole attack.
 - *Black-hole Attack:* A malicious node advertises the wrong paths as good paths to the destination node during the path finding process.
 - *Acknowledgement Spoofing:* An attacker can spoof the acknowledgements of overheard packets destined for particular nodes for providing false information to the neighboring nodes.
 - *Misdirection:* A malicious node sends the packets in the wrong direction from where the destination is unreachable.
 - *Internet Smurf Attack:* The attacker may forge the network and the address of victim and broadcasts multiple messages in the network to flood a victim with hundreds of responses for every request. [3]
 - *Homing:* An attacker identifies traffic pattern and target nodes that have special responsibilities, such as cluster heads or cryptographic- key managers to achieve DoS by destroying these key network nodes. [3]
2. **Denial of service attacks:** This attack is launched by malicious action of some nodes or sudden failure of the nodes in the sensor networks.
3. **Node Subversion:** A normal node can be captured by some attacker node and the attacker may disclose its important security information such as cryptographic keys and thus affects the whole security mechanism of the WSN.
4. **Node Outage:** It is a situation occurred when a normal node stop his functioning. So the WSN must follow an alternative way to handle this situation. As in case, when a cluster head stops its function, then the WSN protocols must be robust enough to handle this node outage problem by using some other suitable route.
5. **Physical Attacks:** WSN works in an open environment due to which they are easily vulnerable to several forms of physical attacks which means threats caused due to physical node destruction.
6. **Node Replication Attacks:** An attacker adds a malicious node in the sensor network by copying the node-id of a normal sensor node.

7. **Passive Information Gathering:** Any opponent having powerful resources can gather information from the sensor networks if sensor node is not encrypted.
8. **False Node:** This situation involves the addition of a false node by an attacker and causes the injection of malicious data in the network.

VII. Attacks in Network Layers and its Defenses

The characteristics of WSN make them susceptible to many new attacks. These attacks can be categorized as- Attacks on secrecy and authentication, Attacks on network availability, Stealthy attacks against service integrity.

A. Physical Layer

Generally, Physical Layer emphasizes on the transmission media between sending and receiving nodes, the data rate, signal strength, frequency types are also addressed in this layer.

1. **Jamming:** It disrupts the entire network or the small portion due to interferences in the radio frequencies and to prevent this attack, spread spectrum techniques and code generation are used.
2. **Radio Interferences:** Large amount of interference is produced either intermittently or persistently. Symmetric key algorithms are used to handle this.
3. **Tampering:** Sensitive information like cryptographic keys or any other data can be extracted by attackers and to prevent this attack, it involves tamper-proofing the node's physical package.

B. Data Link Layer

This layer is responsible for the data frame detection, medium access and multiplexing of data and includes collisions, exhaustion and unfairness attacks.

1. **Collisions:** An attacker may cause collision of packets transmitted on the same frequency and the packets will then be discarded. Error correcting codes are used against this attack.
2. **Exhaustion:** Repeated collision of attacks can cause resource exhaustion which will deplete the energy of surrounding nodes and transmitting nodes. A possible solution is to apply rate limits to the MAC admission control such that network can ignore excessive requests to prevent the energy.
3. **Unfairness:** It is considered as the weak form of a DoS attack. Repeated application of these exhaustion or collision based MAC layer attacks can lead into unfairness. One major defensive measure against such attacks is the usage of small frames, so that any individual node seizes the channel for a smaller duration only.

C. Network and Routing Layer

The attacks occurred in the network layer they are referred as routing attacks. The network and routing layer of sensor networks is usually designed according to the following principles-Power efficiency is an important consideration, Sensor networks are mostly data-centric, and an ideal sensor network has attribute-based addressing and location awareness. There are various attacks occurred at the network layer: - Spoofed, altered and replayed routing information, Sinkhole attack, Black-hole attack, Wormholes etc. All these attacks are explained above under routing attacks. [5]

D. Transport Layer

This layer is used for external networks and to manage the end to end connections. It includes two attacks flooding and desynchronization.

1. **Flooding:** An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach the maximum limit. One solution is to put the limit on number of connections from a particular node.
2. **Desynchronization:** An attacker may repeatedly spoof messages to an end host, causing disruption of an existing connection and missed frames. A possible solution to this type of attack is to require authentication of all packets including control fields communicated between hosts. Header or full packet authentication can defeat such an attack.[7]

E. Application Layer

This layer is in charge of data collection, management and processing of the data by using the application software to obtain trustworthy consequences.

1. **Overwhelm attack:** This attack consumes network bandwidth and drains node energy by overwhelming the nodes causing the network to forward large traffic to the base station. Rate-limiting and efficient data aggregation algorithms can reduce this attack.[5]
2. **Path-Based DoS attack:** This attack can starve the network of legitimate traffic, because it consumes resources on the path to the base station, thus preventing other nodes from sending data to the base station. Combining packet authentication and anti replay protection prevents these attacks. [6]
3. **Deluge (reprogram) attack:** Network programming system let you remotely reprogram nodes in deployed networks. If the reprogramming process isn't secure, an intruder can hijack this process and take control of large portions of a network. It can use authentication streams to secure the reprogramming process. [6]

VIII. Conclusion

Security in sensor networks is a new area of research, with a limited, but rapidly growing set of research results. This paper includes security issues and challenges and defines different security attacks and threats to the sensor networks which may be helpful in order to implement security mechanism. Through this paper, the researchers can understand all the security threats that affect the WSN and researchers can also find out new attacks which affect the WSN security.

References

- [1] Sudhir Agarwal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in WSN" Journal of Computing, Vol. 3, Issue 1, ISSN- 2151-9617, 2011.
- [2] Chaudhari H.C. and Kadam "Wireless Sensor Networks: Security, Attacks and Challenges" L.U. International Journal of Networking Volume 1, Issue 1, 2011, pp-04-16
- [3] Al-Sakib khan Pathan, "Security in wireless sensor networks: Issues and challenges", ICACT2006, ISBN 89-5519-129-4, pp-1043-1048.
- [4] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, "Sensor Network Security: A Survey", IEEE Communications Surveys & Tutorials, Vol. 11, No. 2, Second quarter 2009, pp. 52-73.
- [5] Yong Wang, Garhan Attebury, And Byrav Ramamurthy, "A Survey Of Security Issues In Wireless Sensor Networks" , IEEE Communications Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter 2006.
- [6] Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala, "Security in Wireless Sensor Networks: Issues and Challenges", Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace) 2013, Malaysia, ISSN: 2165-4301, pp. 356-360.
- [7] Sunil Ghildiyal, Ashish Gupta, Musheer Vaqur, Anupam Semwal, "Analysis of Wireless Sensor Networks: Security, Attacks and Challenges", IJRET, Volume 3, Issue 3, eISSN: 2319-1163, pp. 160-164.