Available Online at http://www.journalajst.com

ASIAN JOURNAL OF
SCIENCE AND TECHNOLOGY

ISSN: 0976-3376

Asian Journal of Science and Technology
Vol. 08, Issue, 08, pp.5266-5269, August, 2017

RESEARCH ARTICLE

TYPES OF ATTACKS IN WIRELESS SENSOR NETWORKS: A REVIEW

*K. Chidananda and Dr. K.N. Shreenath

Department of Computer Science and Engineering, Siddaganga Institute of Technology,
Tumakuru-572 103,Karnataka, India

ARTICLE INFO

Article History:
Received 29th May, 2017
Received in revised form
01st June, 2017
Accepted 14th July 2017
Published online 31st August, 2017

Key words:

Security,
Wireless Sensor Network,
Attacks

ABSTRACT

Now-a-days, security is a major concern in every sector. The Wireless Sensor Network is also facing many security problems due to processing power, storage resource, bandwidth and communication ability to expose inside activity and possible attacks. These problems raise serious concerns and points toward necessity to find suitable techniques to provide security to the network. This paper presents various types of attacks on Wireless Sensor Networks.

INTRODUCTION

A Wireless Sensor Network (WSN) is a pool of spatially structured wireless sensor nodes to monitor many variations of eco-friendly circumstances in a helpful mode without trusting on any essential support arrangement (Yun *et al*., 2008).Recently, WSN is being adopted rapidly because of its flexibility and use in several environments. However, sensors in WSN consist of small, inexpensive devices or nodes that have severe limitations like limited processing power, incomplete bandwidth, less storage capability, small battery life and are actually responsible for external threats (Hosam Rowaihy *et al*., 2007) and also Sensor nodes which formsa multi-hop network has a limitation in capacity calculation and energy consumption. When the Base Station (BS) in the network wants to read the sensed information from the network, each sensor node in the network forward its reading to the BS (Sankardas, 2014), possibly via other in-between nodes. This way of reading information from sensor nodes to BS node is too expensive in-terms of communication overhead.WSN provides several benefits such as fast deployment and configuration. At the same time, there are limitations in-terms of sensor nodes, which allow various security threats to the network. These attacks mainly concentrate on nodes by using their limited battery lifetime. In traditional Wired Sensor Network, Public Key Infrastructure (PKI) technique is used for providing security to the sensor nodes to enable data secure communication, but this technique is not suitable for Wireless Sensor Network. When compared to traditional networking system, there are several constraints in the modern wireless sensor networking. In order to enhance security in WSN, it is very important to know about the constraints of the WSN. The main constraints of WSN are storage resource for implementation and limited memory, processing power, Ad-hoc deployment, Hostile Environment, Resource Limitation, Unreliable Transmission, High risk of Physical attack. The model of wireless sensor network is presented in Figure 1.

Limited memory and storage space: Important part of wireless sensor network is sensor node. These nodes are small devices having limited storage capacity. The Size of the program for implementing security for these nodes effectively should be small and hence the size of the Tiny OS will also be small.

Power Constraint: Once sensor nodes are deployed in the WSN, they can’t be replaced because of high operational cost and hence the energy consumed by these nodes is the main constraint in the Wireless Sensor Network. For securing these nodes, extra code is added within these nodes resulting in excess energy consumption by the sensor nodes.

Corresponding author: K. Chidananda,
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumakuru-572 103, Karnataka, India.

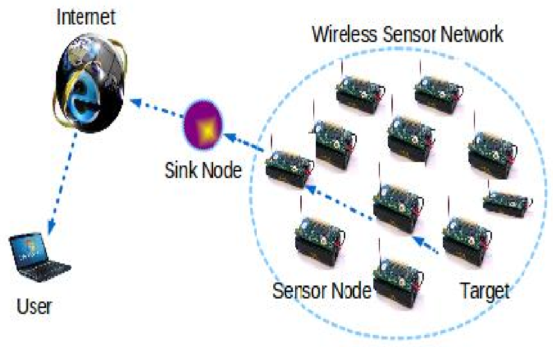

Figure 1.Wireless Sensor Network

Extra code becomes obligatoryfor the purpose of processing of security function, security linked data and store security connected parameters.

Ad-hoc deployment: In WSN, nodes are randomly deployed as there is no proper topological structure of network deployment. In ad-hoc nature of network topology, due to high mobility of nodes, network topology changes frequently. This helps the attacker to attack on the network. Hence security mechanism applied in the network must operate dynamically in association with changes in the nodes.

Hostile Environment: Nodes in the WSN can be deployed in any of the environment. The environment in which nodes are deployed is a challenge. The broadcast mode of transmission medium exposes the network to attack in the form of tampering of the nodes for retrieving information from the nodes. Hence hostile environment is a high research challenge.
Resource Limitation: Resources in WSN are bandwidth, memory and energy required to power nodes. For implementation of security strategies, suitable amount of resource is required, which is limited in wireless sensor nodes. Hence resource limitation is one of the constraints in WSN.

Unreliable Transmission: In WSN, transmission of data is connectionless packet routing and is unreliable.

High risk of Physical attack: Once nodes are deployed in WSN, nodes are left free without control or monitoring of the nodes. This helps the attacker to confront the nodes easily to capture one or more nodes and inject the malicious code into the captured node from the network. This will increase the attacks on the network.

II RELATED WORK

Yi-Sheng *et al.*(2011) concentrated on a mechanism for detection of anomalous moving attackers in sensor network. Based on models of WSN, author presented two different sensing models, namely single-sensing model and multiple-sensing model to derive the detection probability. He also focused on network connectivity and broadcast reach ability. Chun Hu *et al.*(2006) proposed mobile ad hoc network to provide security for applications deployed in this network. Author in this paper introduced a new type of attack named wormhole attack in a mobilead hoc network. In this attack, attacker records packets at one location in the network, passes them to other locations and re-transmit the packets into the network. The main drawbacks of Peer-to-Peer structured network are frequent Sybil attacks to the network because the attackers will generate and controls the huge number of sleuth identities into the network. This will compromise the network to allow an attacker to attack the network. To mitigate Sybil attacks admission controls system is proposed by adaptively constructing a hierarchy of co-operative peers. The Admission control system examines entering nodes via client puzzles in the network. Michael *et al.*(2008) discussed the disadvantage of a traditional wired network and proposed architecture by considering the constraints of the WSN. This architecture forms a topology with the use of the base station to enable peer-to-peer communication between sensor nodes. Further, the topology consists of intermediate nodes for communication if required. Author also provides an algorithm for detection and isolation of anomalous nodes present in the topology.

Attacks on wireless sensor network

Wireless sensor network exposes itself to the attacks by the attacker due the multi-hopnature of transmission medium, deployment of nodes in unprotected environment and no proper layer structure of protocols used in the network. This section summarizes the types of attack in different layers with respect to the ISO-OSI layer model.

Table 1. Types of attack in different layers of OSI model

Layer	Attacks	Security Approaches
Physical Layer	Denial of Service Tampering	Priority Messages Tamper Proofing Hiding Encryption(Abhishek Jain Kamal kant, 2012)
Data Link Layer	Jamming Collision Traffic Manipulation	Use Error Correcting Codes Use Spread Spectrum Techniques
Network Layer	Sybil Attack Wormhole Sinkhole	Authentication Authorization Identity Certificate
Transport Layer	Re-synchronization Flooding	Packet Authentication
Application Layer	Cloning Attack	Cryptographic Approach

Physical layer attacks: Attacks at physical layer of OSI model are called Physical layer attacks. They are

- ***Denial-Of-Service:*** This attack can occur at any layer of the network. The main aim of the attack is to destroy or restructure the network to control or eradicate the functionality of the sensor network.
- ***Tampering:*** In this attack, the attacker confronts the node in the network or destroys a node in the network to introduce a new node by modified malicious code and then insert this node into the network as a new node.

Data Link layer attacks: The possible attacks at Data link layer are

- ***Jamming:*** This type of attack occurs on the availability of sensor nodes. It is caused due to interference with the radio frequency of the network device.
- ***Traffic Manipulation***: The Wireless Communication in WSNs(and other wireless networks)can be easily manipulated in the MAC layer. Attackers can transmit

packets right at the moment when legitimate users do so to cause excessive packet collisions.

- *Collision:* Collision occurs due to pseudo traffic created by the attacker in the transmission line.
- *Exhaustion:* The tampered node in the network frequently sends the info by using power more than required.

Network Layer Attacks: There are two types of attacks namely Passive Attacks and Active Attacks.

Passive Attack: Passive attack means eavesdropping and inspecting the communication channel by an illegal user in the network. Privacy related attacks belong to passive attacks. Sensor nodes in WSN are randomly deployed and independent, i.e. no one has the control on each deployed nodes. This makes attacker to access a huge volume of information from the nodes remotely. Some of the common attacks (Undercoffer, 2002) are mentioned below:

- Monitor and Eavesdropping
- Traffic Analysis
- Camouflage Adversaries

- **Monitor and Eavesdropping:** It is concerned with the data about the control information of the sensor network configuration. The attacker easily finds the communication information from snooping.
- **Traffic Analysis:** Even though the data in the sensor nodes are encrypted, they can be captured by the attackers by Traffic Analysis which can cause harm to the network.
- **Camouflage Adversaries:** Attacker easily compromises the sensor nodes in the WSN. Then the attacker can insert or copy a malicious node into the network.
- ***Active Attack:*** Active attack means monitoring, listening, modifying the information in the communication channel by unauthorized user to a network.

Few of the active attacks are mentioned below:

- Routing Attacks in Sensor Networks
- Selective Forwarding
- Sinkhole Attack
- Sybil Attack
- Wormhole Attack
- HELLO Flood Attack
- Node Subversion
- Node Malfunction
- Node Outage
- Physical Attacks
- Message Corruption
- False Node
- Node Replication Attacks

Routing Attacks in Sensor Networks:

Attacks occurring at the network layer of the protocol are called Routing Attacks (Wood, 2002) as shown in Figure 2.Some of the Routing Attacks are spoofing, altering and replaying routing information. An unprotected ad hoc routing is vulnerable to these types of attacks, as every node acts as a router, and can therefore directly affect routing informationas shown in Figure 3.

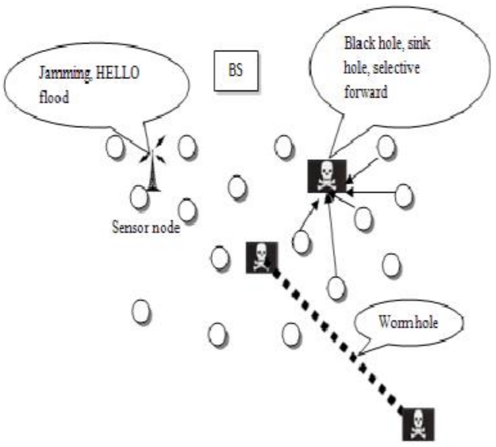

Figure 2. Routing attacks in WSN

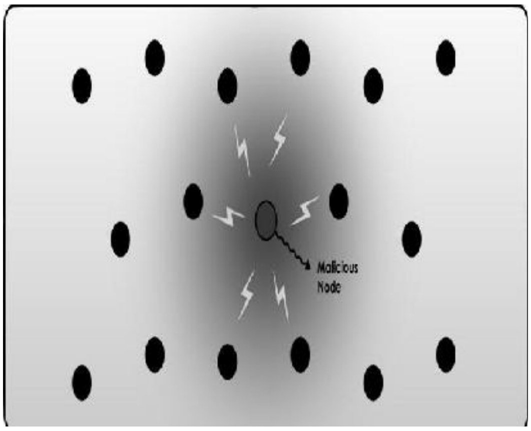

Figure 3. Spoofing of nodes in WSNs

Selective Forwarding: The data is transmitted to the sink node by forwarding data from the source to selected node in sensor network. It is assumed in the networking that node faithfully forwards data from one node to another node. In the case of attack, the attacker selectively captures a node in the network and this node rejects to advance the packet to the next node. In this situation, neighboring node takes different path to forward the packet (Chris Karlof, 2014). Selective forwarding is pictorially represented as shown in Figure 4.

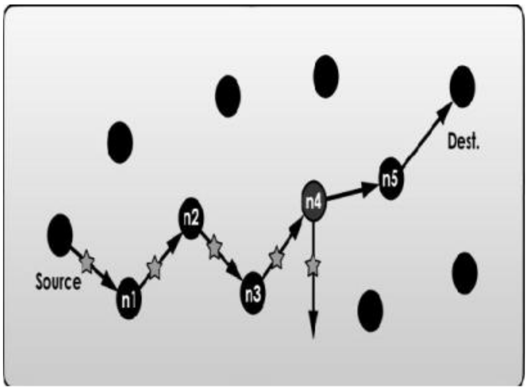

Figure 4. Selective Forwarding in WSNs

- **Sinkhole Attack:** The main goal of the attackers is to attack on all traffic information to reach the sink node by compromised node (Chris Karlof, 2003).

- **Sybil Attack:** Few attacks target fault-tolerance by generating single node multiple identities in the network.
- **Wormhole Attack:** In this attack, attacker records one packet at one location and modifies the packet and then shifts them to another location and retransmits them into the network.
- **HELLO Flood Attack:** In WSN, the source node sends Hello message to its entire neighbor for their identification. The Attacker will transfer the Hello message with the high radio transmission range. While transferring packets, the nodes feel the attacker node as its neighbor node and transfer packets through it.

- **Node Subversion:** Attacker capture sensor nodes and gathers information about cryptographic keys and other secure details about the data stored.
- **Node Malfunction:** Node Malfunction means modifying the node information or keeping malicious code in the compromised node resulting in inaccurate data. The corrupted data will expose integrity of a sensor network (Pathan, 2006).
- **Node Outage:** This is a situation where the node stops functioning due to which the cluster node also stops working.
- **Physical attack:** Physical attack means destroying a node in the network because nodes in the network are deployed in hostile environment. This will helps the attacker to perform above mentioned attacks.
- **Message Corruption:** Message corruption means modifying the original message by the attacker. This will be achieved by the attacker by compromising the node in the network. It will affect the integrity of the network.
- **False Node:** False node is a node introduced into a sensor network by the attacker to corrupt original data. This will stop transmitting the original data to the network.
- **Node Replication attacks:** This attack concentrates on the performance of the network. This is called Node replication attack as it results in detached network, corrupted data reading by nodes in the network.

Transportation layer Attacks

- ***Resynchronization Attack:*** In this attack, the sequence number is modified by the attacker in which, packet disturbs the topology of the network communication.
- ***Flooding Attack:*** By this attack the server gets down due to flooding of large amount of traffic. In which, it results in the memory buffer to become full. Once the server buffer fills, the connection to the server gets failed. This is also a type of Denial-Of-Service attack.

Application layer Attacks

Cloning Attack: In WSNs, attacker easily compromises the sensor node in the network and then the attacker can deploy any number of clone nodes i.e. malicious nodes into the network. These malicious nodes can capture or gather all information of nodes in the network and can modify it. These nodes act as legitimate nodes of the network. If clone nodes are not detected in the network, it makes the sensor network undefended to attacks.

Conclusion

Wireless sensor network is a very useful network. Now-a-days every one prefers WSN for many applications, for example smart parking. Though WSNs provide many advantages, there are some disadvantages also. The main challenge in WSNs is security. Since nodes in the network are deployed in hostile environment, have no proper topology on the network for data transmission, routing is also independent, no proper monitoring of sensor nodes in the network, the network is exposed to attack in many ways. Hence it requires a secure mechanism to avoid the attacks by the attacker. In this paper, various types of attacks in the Wireless Sensor Network are briefly discussed.

REFERENCES

Yun Wang, xiaodong Wang, Bin Xie. 2008. "*Intrusion detection in Homogeneous and heterogeneous wireless sensor Networks*",IEEE Transaction on Mobile Computing, Vol.7.

HosamRowaihy, William Enck*"Limiting Sybil Attacks in Structured P2P Network"*,June 2007, INFOCOM 2007, 26th IEEE International Conference on Computer Communications, IEEE:06/2007, DOI:10.1109/INFCOM.2007.328.

Sankardas Roy, Sanjeevsetia, 2014. "*Secure Data Aggregation in Wireless Sensor Network*", IEEE Transactions on Information Forensics and Security, Vol. 9.

Yi-Sheng Shiu , Shih yuchang, 2011. "*Physical layer security in Wireless Sensor Network*", IEEE Wireless communication, Vol.18, Issue 2.

Yih-Chun Hu, Adrian perrig, David B, Johnson, 2006. "*Wormhole Attacks in Wireless Network*", IEEE Communications, Vol.24, Issue 2.

Michael Collins, SimonDobson, Paddy Nixon, 2008. "*Lightweight Secure Networks*", J.Internettechnology and secured transactions, Vol. 10, Issue 10.

Abhishek Jain Kamal Kant 2012."*Security solutions for Wireless Sensor Networks*",IEEE Conference on Advanced Computing & Communication Technologies.

Undercoffer, Avancha, Joshi, 2002."Security for sensor networks", pp.1-11.

Chris Karlof, David Wagner, 2003. "*Secure Routing in Wireless sensor networks: Attacks and Countermeasures*", Ad-hoc networks, pp.299-302

Wood, A.D. & J. A. Stankovic, 2002. "*Denial of Service in Wireless sensor network*", IEEE, Vol.35, Issue.10, pp.54-56,

Pathan, A.S.K. 2006."*Wireless Sensor networks: Issues and Challenges*", ICACT, pp. 1-6.

Al-sakib Khan Pathan, Hyung-Woo Lee, 2006. "*Wireless Sensor Networks: Issues and Challenges*", ICACT, ISBN: 89-5519-129-4-1043, pp.20-22

Manjuprasad B, Andhe Dharani, 2014."*Simple Secure protocol for Wireless Sensor Network*".

****