International Journal of Future Generation Communication and Networking
Vol. 8, No. 4 (2015), pp. 81-88
http://dx.doi.org/10.14257/ijfgcn.2015.8.4.08

Review on Security Issues and Attacks in Wireless Sensor Networks

Lovepreet kaur and Jyoteesh Malhotra

CSE Dept. GNDU Regional Campus Jalandhar.
Lovebatala@gmail.com.

Abstract

Wireless sensor network is a collection of sensor nodes with limited processor and limited memory unit embedded in it. Sensor networks are used in wide range of applications such as Environment monitoring, health, industrial control units, military applications and many more. This paper defines the security requirements and various attacks on sensor network. This paper also review proposed security mechanisms for WSN.

Keywords: *Wireless sensor network, Security, Attacks, Security Mechanisms.*

1. Introduction

WSN's are hub of small sensor nodes with low power, low bandwidth and small processing capabilities. Usually sensor node processor is of 4-8 MHz, 4 kb of RAM and 128KB flash. In WSNs sensor node basically sense data, collect data from other nodes then process that data and then transmit that collected data to the base station. As security is main concern in any network but in case of sensor network security of data is a big challenge because in sensor network we can't apply heavy algorithms for security because of low power/battery and low memory of sensor nodes. Wireless network is more prone to attacks than wired and traditional security techniques in computer networks are not applicable to WSN's. In case of multihop communication in wireless sensor network wireless medium is unreliable in communication and insecure. Already researchers have done work in area of security of sensor network through cryptography and to save energy (through LEACH, PEGASIS and HEED protocols).Contrary of this many attacks are designed to exploit the unreliable communication channels. In wireless sensor network no fixed deployment pattern is used because deployment of sensor nodes change according to the application for which it is to be used and unreliable communication channel, so it is more prone to different security attacks. Sensor nodes are usually deployed in accessible areas so more vulnerable for physical attacks. Sensor nodes are deployed in physical environment more close to people posing new security problems. There is a probability of capturing sensor nodes by adversaries and attackers may change the internal program and gain the whole control of network and get all the confidential information and launch various malicious attacks on the hacked or compromised nodes.

In this paper section 2 and 3 describe security requirements for sensor networks, in section 4 list of various attacks on sensor network, in section 5 corresponding defensive measures. At the last in section 6 paper is concluded.

2. Security Requirements

Wireless sensor networks are quite different from other wireless and wired networks. Security is very important in wireless communication as sensor nodes are deployed in real environment so easily vulnerable to different types of attacks and threats. For critical wireless sensor application security is main focus due to in real environment deployments

ISSN: 2233-7857 IJFGCN

of nodes hacker attack the sensory nodes and will get the access to the data or may change the real data with false data/wrong information to the base station for false analysis of environment data. The security services should protect the information communicated over network and to protect sensor nodes from physical attacks or internal attacks. There are some security properties applicable to each sensor networks which are listed below.

2.1. Data Confidentiality

Data confidentiality is a vital part in wireless sensor network. The information which is passing through the network must be confidential. Sensor node information like its sensors identities and keys that are public should be protected using different algorithms like cryptography to ensure the data confidentiality. Sensor nodes communicate very sensitive data so its confidentiality is very important, sensor network should not leak its sensitive readings to the neighboring networks. The standard approach to encrypt data is to encrypt the sensitive data so that only intended users will get the information.

2.2. Data Authentication

Authentication is required in many administrative tasks like reprogramming in sensors and controlling sensor node duty cycle. An adversary can inject message to any sensor node so the sensor node authenticate it that whether it is correct source or not. Various authentication mechanisms are used like digital signature, cryptography to ensure that sender node is authenticated node.

2.3. Data Integrity

As in sensor network data may be altered by using compromising nodes so integrity controls must ensure that data received has not been altered until it reaches its original destination. Adversary can change the data through malicious node and change the packet data before its destination and may send false information to the receiver.

3. Security Requirements in Secure Sensor Network

As above defined requirements are basic requirements for WSNs despite all many more requirements are needed for sensor network security above basic requirements cannot to be enough for sensors security. These requirements are as follows:

3.1. Data Freshness

Data freshness in sensor network means data is recent and not replaying (repeated packet) as adversary can jam the network through compromising nodes or by sending same data through the network nodes in order to deplete the energy of sensor nodes it means if particular node is sending same data packet because of malicious attack that nodes energy depleted and node will die. Data freshness also ensures ordering facility. Various security protocols are designed to ensure that data is fresh and if it is duplicated data node simply discard that data to avoid JAMMING in network.

Key establishment ensures that session is fresh. It is basically in two forms weak and strong key for data freshness security. In weak ordering of packets is partial but carry no delay information and it is used by sensor measurements and strong freshness provide ordering facility on request-response pair and allow for delay estimations used for time synchronization in network.

3.2. Self Organization

As WSNs has no fixed infrastructure as WSNs are Ad- hoc networks. So sensor nodes must be independent and flexible enough to be self organizing and self-healing according to different conditions because in sensor network once we deploy the sensor nodes we are not able to manually organize node in any situation like in case of satellites. So sensor nodes must be self organizing on the basis of secure key management nodes will get their position in network through the neighboring nodes or through GPS (global positioning system). After the failure of any node in the network new node will replace the failure node through self organizing mechanism so that network will not effected.

3.3. Scalability

For large or densely deployed networks number of sensor nodes is in order of 10 to 10,000 nodes. In such a large network only some nodes are power or energy rich for transmission. With the failure of any node new node cope with all the other network nodes and key management should cope with the scalability of network size. In distributed sensor networks key management is done by dividing the large network into subgroups and security is provided through re-encrypt messages when they are forwarded to another group. This mechanism is useful where transmission energy cost is important the computation cost.

3.4. Availability

Availability of nodes means the life time of nodes. To secure the availability of nodes network should protect the sensor nodes from idle listening or unnecessary processing to save energy of sensor nodes. Various routing protocols (LEACH, SPIN, GEAR, PEGASIS, HEED) are used to save energy and extend the life of network [7].

3.5. Time Synchronization

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pairwise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc. [8], proposes a set of secure synchronization protocols for sender-receiver (pairwise), multi-hop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization

3.6. Accessibility

Intermediate nodes accessibility must be provided through key management system. As if node to node confidentiality should provided it may prevent the data fusion by each sensor node, so each node in its network access the sensor data of another node through some defined key procedure like direct or transitive key management schemes. In case of direct key all the sensor network nodes have single network key for all the sensor nodes and in transitive key management scheme each node has different key to decrypt/verify the received data and another key to again re-encrypt the data which is to be forwarded to next node. This key scheme is used for small groups

4. Types of Attacks on Sensor Network

Wireless sensor networks are vulnerable to various attacks like on nodes, network and on sensed data also. This section explains various types of attacks on sensor network.

4.1. Attacks at Different Layers

Physical attack discussed in introduction section adversely affect the sensor network beside this attack number of attacks affect the different layers of wireless sensor network. This section explores the list of different attacks at different layers of WSNs

4.1.1. Physical Layer

Actual data transmission, frequency generation, data reception, carrier frequency selection, signaling, encryption and the transmission media done at physical layer. WSNs generally use radio based and shared transmission medium. Attacks at physical layer are

4.1.1.1. Jamming

Jamming is a common attack at physical layer by just tracking the radio frequency range used for WSN data transmission. Acc to [2] adversary continuously send signals of same frequency as that of sensor node. This radio signal interferes with original signal sent by the sender node and the receiving node will not get any signal because of the interference created by the attacker. So that the affected node completely separated by the attacker from sensor network.[3] jamming is such a powerful that it will adversely affect the whole network and even attacker can jam the whole network message by distributing different jamming sources/devices. These leads to Denial-of-service attack in this attack attacker violate the communication protocol. By jamming the message exchange between network and increase the number of collisions hence retransmission of data depletes the energy of particular node and life time of network depleted.

4.1.1.2. Tampering

Sensor nodes are deployed in unattended environment so highly susceptible to physical attacks it adversely affects the node by capturing the node and access cryptographic keys, tamper with its circuit, change internal program and get all access of node and tamper whole network communication.

4.1.2. Link Layer

This layer is responsible for multiplexing of data stream, error control, medium access and data frame detection. It is vulnerable to collision when more then one sender tries to send data on single medium [2].Attacker transmit data with same frequency and increase collision in the network and re-transmission of same data violates the energy of particular node and exhaust resources. Unfairness is a weak form Denial-of-service attack. These attacks occur at data link layer.

4.1.3. Network Layer

In network layer routing of packets is the main task, packets are routed from node to base station, node to cluster head or to neighbor node. This layer is very important in WSN, for energy efficient routing mechanisms. Attacks at network layer are

4.1.3.1. Selective Forwarding

In network where messages are forwarded to other nodes like in WSN, this attack occurs. In this attack, adversary attack on particular node in such a way that node forward only selective messages and drop other messages. This attack is basically done on those nodes which are close to the sink node because all other messages route through these nodes in this way all important messages dropped. Such type of attacks commonly used in

military application and on those applications where correct information is important. This leads to worse when adversary changes the traffic route.

4.1.3.2. Sinkhole Attack

As the name of this attack suggests, that adversary create a sink node in such a way that it attracts all neighbor nodes to send their data to that node and it helps in selective forwarding, adversary get the control of all information.

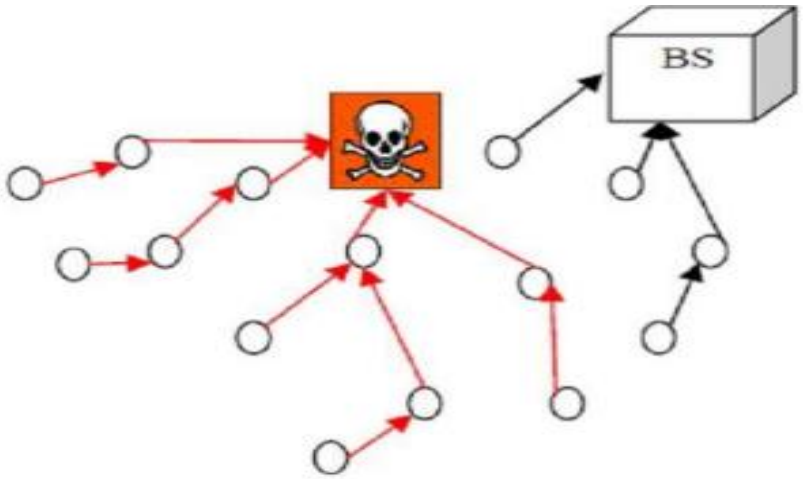

Figure 1. Black Hole Attack in WSN

4.1.3.3. Wormhole Attack

This attack is listed as a most complicated attack in wireless sensor network. In this attack adversary creates a low link tunnel between the nodes and replays all messages. All the data get transmitted through this tunnel. This attack is a combination of other attacks like sinkhole attack, by creating tunnel adversary will broadcast the route establishment message to all other nodes. It is used to exploit the routing in the network by sending data to the false destination instead of original destination [3].

4.1.3.4. Hello Flood Attack

As the name suggests in this attack adversary broadcast the hello message to the whole network and attract other nodes to choose this route for their message transmission. In this attack adversary sends high power message to other nodes and nodes believe that they are in the range of that node and assume adversary's node as a neighbor node and send their information to that node and waste their power.

4.1.3.5. Sybil Attack

This attack target the location based routing techniques where messages passes on the basis of geographical location. In this attack fake identity of node is created that means same node is present on different places in the network, create false route for the transmission of information and violates the routing algorithms and fairness of the network.

4.1.4. Transport Layer

There are two basic attacks on this layer

4.1.4.1. Flooding Attack

Adversary at this layer exploits the protocols that maintain the state at either end of the connection [4]. Adversary send many requests to the targeted node for connection establishments and while doing so the exhaust its resources.

4.1.4.2. De-synchronization

In this attack adversary attack on active connection, adversary changes the sequence number and control flag of active connection either at one end or both. In this way adversary desynchronize the connection for this reason sensor node retransmit the messages and their energy is wasted.

5. Defenses Against Attacks on Sensor Network

5.1. Physical Layer

- **Jamming Attack defence:** For jamming attacks various frequency hopping techniques are used like spread spectrum etc. but not suitable for wireless sensor network as it require large amount of processing power and battery. For this Ultra Wide Band is used as anti jamming technique, a very short pulse is seeded on wide frequency band which is very difficult for adversary to detect.

5.2. Data Link Layer

- **Denial of services:** Various error correcting codes are used to avoid collisions but not suitable for wireless sensor network due to limited memory and power. Various encryption techniques are used like Tiny Sec etc.

5.3 Network Layer

- ***Selective forwarding:*** For this attack, detection of malicious node which is behaving in different ways is done and another route is chosen for transmission or data is transmitted on multiple paths.
- **Sink hole and warm hole:** These attacks are very difficult to detect but using geographic based routing malicious node will be detected and nodes are aware of their location hence these attacks avoided.

- **Hello attack:** Excess of route establishment message by adversary malicious node is avoided by using authentication process of sender node like μTESLA based cryptography techniques.
- **Sybil attack:** Verification of nodes is necessary to avoid this type of attack so using hash function each node is assigned with unique key, which is used in transmission for verification purpose.

5.4 Transport Layer

- **Flooding and De-synchronization:** Flooding attack can be avoided by limiting the connection of a node but it will not suitable for sensor networks to limit the nodes connectivity. Another method used is client puzzle when node wants to connect with other node it must solve puzzle. For de-synchronization attack authentication of packets is important between two nodes during active connection, for this transport layer's header and control fields must be authenticated.

6. Conclusion

Wireless sensor network is used in different types of applications due to tremendous growth. Hence security and reliability becomes the main concern in every wireless sensor network applications. This paper presents survey on different types of attacks possible on different layers of network and list possible defenses against them. Security defenses must be strong enough to avoid adversary to affect the network, as wireless network is more prone to attacks, it is necessary to handle the data with full confidentiality and with high security but due to its small battery capacity and limited memory for processing restricts against the heavy security algorithms but it still needs the small and efficient techniques to secure its data communication over wireless medium and to save energy (battery life) also.

Acknowledgements

First of all I would like to thank Dr. Jyoteesh Malhotra for his support and valuable suggestions during the whole research process. No one can perform better without proper guidance. Further I am thankful to all faculty members and staff of department of computer science and engineering. Last but not the least I would like to thank my family members for their constant motivation and support.

References

[1] G. Bianchi, "A comparative study of the various security approaches used in wireless sensor networks,"International journal of advanced science and technology, vol.17, **(2010)**, pp.31-44.
[2] J. Sen, "A Survey on wireless sensor network security", vol.1, no.2, **(2009)**.
[3] J. Rehana, "Security of wireless sensor network", TKK T-110.5190 Seminar on Inter networking, **(2009)**.
[4] M. Sharifnejad and M. Sharifi, "A survey on wireless sensor networks security", 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, **(2007)**; TUNISIA.
[5] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks an countermeasures ", Ad Hoc Networks, vol.1, **(2003)**, pp.293–315.
[6] A. Singla and R. Sachdeva, "Review on Security Issues and Attacks in Wireless Sensor Networks", IJARCSSE, vol.3, no.4, **(2013)**.
[7] Lovepreet, "Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey", International Journal of Computer Applications (0975 – 8887)vol.100, no.1, **(2014)**.
[8] B. Parno, A. Perrig and V. Gligor, "Distributed detection of node replication attacks in sensor networks", In Proceedings of IEEE Symposium on Security and Privacy, **(2005)**.
[9] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks", IEEE Computer, vol.35, no.10, **(2002)**, pp.54 -62.
[10] M. Chowdhury, M. Fazlul Kader and Asaduzzaman, "Security issues in wireless sensor networks:A Survey", International Journal of Future Generation Communication and Networking, vol.6, no.5, **(2013)**, pp.97-116.
[11] M. A. Abuhelaleh and K. M. Elleithy, "Security in Wireless Sensor Networks: key Management Module in SOOAWSN", International Journal of Network Security & Its Applications, vol.2, no.4, **(2010)**.
[12] A. S. Pathan, H. W. Lee and C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges", **(2006)**.
[13] M. A. Abuhelaleh and K. M. Elleithy, International Journal of Network Security & Its Applications, vol.2, no.4, **(2010)**.

Authors

Lovepreet kaur, she was born in Batala city, state Punjab in INDIA during 9 Nov 1990. She completed Btech with Distinction from SSCET badhani, Pathankot and M.Tech from Guru Nanak Dev University (GNDU) RC Jalandhar during 2013-2015. Her research interests are in the broad area of QoS aware convergecast routing in wireless sensor network. She has published papers in scientific journals and also presented in international conferences. Contact email lovebatala@gmail.com