Attacks in Wireless Sensor Networks and Security Measures

Reema Sandhu
Assistant Professor(Comp Sci)
Dr. B.R.A. Govt College
Kaithal(Haryana)India

Abstract:- Wireless Sensor Networks(WSNs) consists of low power, low-cost smart devices which have limited computing resources. With a widespread growth of the applications of WSN, the security mechanisms are also be a rising big issue. A lot of real world applications have been already deployed and many of them will be based on wireless sensor networks. These applications include geographical monitoring, medical care, manufacturing, transportation, military operations, environmental monitoring, industrial machine monitoring, and surveillance systems. This paper discusses security goals, constraints and typical attacks along with their defensive techniques or countermeasures relevant to the sensor networks. Some network security measures in case of wireless sensor networks followed by conclusion are also stated

Keywords – Attacks, Security, Sensor nodes, Wireless Sensor Network.

INTRODUCTION

Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors. The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Today's sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties. In case of wireless sensor network, the communication among the sensors is done using wireless transceivers. Basically the major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensors.

GOALS

The primary goals of security in WSN are to provide:

- **Confidentiality** – Data being transported in the network cannot be read by anyone but the intended recipient.
- **Integrity** – Any message received is known to be exactly the message that was sent, without additions, deletions or modifications of the content.
- **Authenticity** – A message that claims to be from a given source is, in fact, from that source. If time is used as part of the authentication scheme, authenticity also protects a message from being recorded and replayed.
- **Data Availability-** Availability is of importance for maintaining an operational network. It is the ability of a node to utilize the resources and the network is available for the message to move on.
- **Data Freshness -** It ensures that data contents are recent and there no replay of any old content. This requirement is especially important when there are shared-key strategies employed in the design and need to be changed over time.
- **Self-Organization:-** WSN is typically an ad-hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the network management, so nodes must their selves adapt the topology and deployment strategy.

- **Time Synchronization:-** Many WSN applications demand some form of time synchronization for execution. A more collaborative sensor network may require group synchronization for tracking applications.
- **Secure Localization:-** Sensors may get displaced while deploying them or after a time interval or even after some critical displacement incident. The utility of a WSN will rely on its ability to accurately and automatically locate each sensor in the network.

CONSTRAINTS IN WSN

- **Limited Resource :-**Sensor nodes have limited resources, including low computational capability, small memory, low wireless communication bandwidth, and a limited, usually no rechargeable battery.
- **Small message size:** Messages in sensor networks usually have a small size compared with the existing networks. As a result, there is usually no concept of segmentation in most applications in WSN.
- **Local Addressing Schemes:** Due to relatively large number of sensor nodes, it is not possible to build global addressing schemes for deployment of a large number of sensor nodes as overhead of identity maintenance is high.
- **Sensor location and redundancy of data:** Position awareness of sensor network is important since data collection is normally based on location. Also there may be common phenomena to collect data, so there is a high probability that this data has some redundancy.

WSN ATTACKS

WSNs are organized in layered form. This layered architecture makes these networks vulnerable to various kinds of attacks.

Denial of Service Attack

In the denial-of-Service(DoS) attack, the hackers's objective is to render target machines inaccessible by legitimate users. Dos attacks can happen in multiple WSN protocols layers. . They mainly attack Physical, Link, Network, Transport layers At physical layer, the DoS attack could be jamming and tempering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer, this attack could be performed by malicious flooding and desynchronization.

Defense Mechanism:- The mechanisms to prevent DoS attacks include payment for resources, pushback, strong authentication and identification of traffic .One security technique uses authentication streams to secure the reprogramming process. This divides a program into a series of messages, each of which contains a hash of the next message. This mechanism ensures that an intruder can't hijack an ongoing program transmission, even if he or she knows the hashing mechanism. This is because it would be almost impossible to construct a message that matches the hash contained in the previous message. A digitally signed advertisement, which contains the program name, version number, and hash of the first message, ensures that the process is securely initiated. Many threats can be identified using existing encryption and authentication mechanisms, and other techniques (such as identifying jamming attacks) can alert network administrators of ongoing attacks or trigger techniques to conserve energy on affected devices.

Sinkhole attacks:-

In sinkhole attacks, adversary attracts the traffic to a compromised node. The simplest way of creating sinkhole is to place a malicious node where it can attract most of the traffic, possibly closer to the base station or malicious node itself deceiving as a base station. One reason for sinkhole attacks is to make selective forwarding possible to attract the traffic towards a compromised node. The nature of sensor networks where all the traffic flows towards one base station makes this type of attacks more susceptible. They mainly affect Link layer, Network layer

Defense Mechanism:- Such attacks are very difficult to defend against. One class of protocols resistant to these attacks is

geographic routing protocols. Geographic protocols construct a topology on demand using only localized interactions and information and without initiation from the base station.

Sybil attacks:-

In a Sybil attack, a single node presents multiple identities to other nodes in the network. A node can pretend to be more than one node using the identities of other legitimate nodes .This type of attack where a node forges the identities of more than one node is the Sybil attack. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. By using the Sybil attack an adversary can "be in more than one place at once".

Defense Mechanism:- The mechanisms to prevent against Sybil attacks are to utilize identity certificates . The basic idea is very simple. The setup server, before deployment, assigns each sensor node some unique information. The server then creates an identity certificate binding this node's identity to the assigned unique information, and downloads this information into the node. To securely demonstrate its identity, a node first presents its identity certificate, and then proves that it possesses or matches the associated unique information. This process requires the exchange of several messages

Selective forwarding

Multi-hop networks are often based on the assumption that participating nodes will faithfully forward received messages. In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet it sees. However, such an attacker runs the risk that neighboring nodes will conclude that she has failed and decide to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a selected few nodes can reliably forward the remaining traffic and limit suspicion of her wrongdoing. Selective forwarding attacks are typically most effective when the attacker is explicitly included on the path of a data flow. However, it is conceivable an adversary overhearing a flow passing through neighboring nodes might be able to emulate selective forwarding by jamming or causing a collision on each forwarded packet of interest. The mechanics of such an effort are tricky at best, and may border on impossible.

Defense Mechanism:- Multipath routing can be used to counter these types of selective forwarding attacks. Messages routed over paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most compromised Allowing nodes to dynamically choose a packet's next hop probabilistically from a set of possible candidates can further reduce the chances of an adversary gaining complete control of a data flow.

Wormhole Attack:-

Wormhole attack is one of the attacks on the network layer attack that can affect the network routing, data aggregation and location based wireless security even without the knowledge of cryptographic techniques implemented. This is the reason why it is very difficult to detect. It is caused by one, two or more number of nodes in which two attacker nodes creates a link call i.e. the wormhole link by which both the nodes can communicate. These nodes give an illusion that the selected path is a shortest path to get the destination. In most commonly type of two ended wormhole, one end tunnels the packets via wormhole link and the other end, on receiving packets, replays them to the local area. Wormholes are hard to detect because they use a private, out-of-band channel which is invisible to the WSN. Packets are forwarded between the malicious nodes by encapsulation and use of additional hardware such as a wired link or a directional antenna. Wormhole attacks are more likely be used in combination with selective forwarding or eavesdropping . The wormhole attack is especially difficult to detect in WSNs when using routing protocols in which routes are decided based on advertised information such as minimum hop count to base station.

Defense Mechanism:-Majority of the techniques presented require additional

hardware support, tight time synchronization, localization information or may be confined to specific routing algorithm**.**

HELLO flood attacks:-

Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor. For example, an adversary advertising a very high quality route to the base station to every node in the network could cause a large number of nodes to attempt to use this route, but those nodes sufficiently far away from the adversary would be sending packets into oblivion. The network is left in a state of confusion. A node realizing the link to the adversary is false could be left with few options: all its neighbors might be attempting to forward packets to the adversary as well. Protocols which depend on localized information exchange between neighboring nodes for topology maintenance or flow control are also subject to this attack. An adversary does not necessarily need to be able to construct legitimate traffic in order to use the HELLO flood attack. She can simply re-broadcast overhead packets with enough power to be received by every node in the network. HELLO floods can also be thought of as one-way, broadcast wormholes.

Defense mechanism:- This can be avoided by checking the bidirectional of a link, so that the nodes ensure that they can reach their parent within one hop.

Passive Information Gathering

An intruder with an appropriately powerful receiver and well designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields

Defense mechanism:- To minimize the threats of passive information gathering, strong encryption techniques need to be used.

NETWORK SECURITY SERVICES

Some high-level security mechanisms for security of wireless sensor networks are discussed below .

Grouping of sensor nodes :-Each node in a wireless sensor network is limited in its computing and communication capabilities. However, interesting in-network data aggregation and analysis can be performed by groups of nodes. For example, a group of nodes might be responsible for jointly tracking a vehicle through the network. The actual nodes comprising the group may change continuously and quickly. Many other key services in wireless sensor networks are also performed by groups. Consequently, secure protocols for group management are required, securely admitting new group members and supporting secure group communication. The outcome of the group's computation is normally transmitted to a base station. The output must be authenticated to ensure it comes from a valid group. Any solution must also be efficient in terms of time and energy (or involve low computation and communication costs), precluding many classical group-management solutions.

Intrusion detection*:-* Wireless sensor networks are susceptible to many forms of intrusion. In wired networks, traffic and computation are typically monitored and analyzed for anomalies at various concentration points. This is often expensive in terms of the network's memory and energy consumption, as well as its inherently limited bandwidth. Wireless sensor networks require a solution that is fully distributed and inexpensive in terms of communication, energy, and memory requirements. In order to look for anomalies, applications and typical threat models must be understood. It is particularly important for researchers and practitioners to understand how cooperating adversaries might attack the system. The use of secure groups may be a promising approach for decentralized intrusion detection.

Aggregation of data:- One benefit of a wireless sensor network is the fine-grain sensing that large and dense sets of nodes

can provide. The sensed values must be aggregated to avoid overwhelming amounts of traffic back to the base station. For example, the system may average the temperature or humidity of a geographic region, combine sensor values to compute the location and velocity of a moving object, or aggregate data to avoid false alarms in real-world event detection. Depending on the architecture of the wireless sensor network, aggregation may take place in many places in the network. All aggregation locations must be secured. If the application tolerates approximate answers, powerful techniques are available; under appropriate trust assumptions, randomly sampling a small fraction of nodes and checking that they have behaved properly supp supports detection of many different types of attacks.

Conclusion

Security in Wireless Sensor Network is vital to the acceptance and use of sensor networks. The challenges of Wireless Sensor Networks are also briefly discussed. In particular, Wireless Sensor Network product in industry will not get acceptance unless there is a full proof security to the network. This paper summarizes the attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanism widely used to handle those attacks and network security services has been discussed for security of wireless sensor networks.

REFERENCES

[1] X. Du, and H-H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications, vol. 15, no. 4, Aug. 2008, pp.60-66.

[2]Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks, " IEEE Commun. Surveys Tutorials, vol. 8, pp. 2– 23, year 2006
.

[3]A.D. Wood and J.A. Stankovic, (2002) "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, 2002, pp. 54– 62.

[4] Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688

[5] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks", CADIP Research Symposium, 2002, available at, http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf

[6] Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003). vol.1, pp. 335 - 340.

[7] J. R. Douceur,(2002) "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS‟02).

[8] Zaw Tun and Aung Htein Maw,(2008)," Worm hole Attack Detection in Wireless Sensor networks", proceedings of world Academy of Science, Engineering and Technology Volume 36, December 2008, ISSN 2070-3740.

[9]. Zhou, L. and Haas, Z. J., "Securing ad hoc networks", IEEE Network, Volume 13, Issue 6, Nov.-Dec. 1999, pp. 24 – 30.

[10] Karlof, C., Wagner, D (2003) "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Ad-Hoc Networks 1(3), 293-315.