IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 12, December 2015.
www.ijiset.com
ISSN 2348 – 7968

Wireless Sensor Network's Challenges and Attacks- a Comprehensive Study

Gurmukh Singh
Assistant Professor
UIET, Panjab University
Chandigarh
Email: gurmukh86@gmail.com

Rajneesh Singla
Assistant Professor
UIET, Panjab University
Chandigarh
Email: eng.singla85@gmail.com

Abstract: Wireless sensor network applications include ocean and wildlife monitoring, manufacturing machinery performance monitoring, building safety and earth-quake monitoring, and many military applications. Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks and a brief study about various attacks of wireless sensor networks.

Keywords: DoS attack, WSN, Security,

1. INTRODUCTION

A wireless sensor network consists of a large number of nodes spread over a specific area where we want to look after at the changes going on there [2]. A sensor node generally consists of sensors, actuators, memory, a processor and they do have communication ability. All the sensor nodes are allowed to communicate through a wireless medium. The wireless medium may either of radio frequencies, infrared or any other medium, of course, having no wired connection. These nodes are deployed in a random fashion and they can communicate among themselves to make an ad-hoc network [7]. If the node is not able to communicate with other through direct link, i.e. they are out of coverage area of each other, the data can be send to the other node by using the nodes in between them. This property is referred as multi-hoping . All sensor nodes work cooperatively to serve the requests. Generally WSNs are not centralized one as there is peer-to-peer communication between the nodes. So there is no requirement of prior established infrastructure to deploy the network. 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 [4].In case of wireless sensor network, the communication among the sensors is done using wireless transceivers.

2. CHARACTERISTICS

It includes two kinds of nodes:

- Sensor nodes with limited energy can sense their own residual energy and have the same architecture.
- One Base Station (BS) without energy restriction is far away from the area of sensor nodes.
- All sensor nodes are immobile. They use the direct transmission or multi-hop transmission to

ISSN 2348 – 7968

communicate with the base station.

- Sensor nodes sense environment at a fixed rate and always have data to send to the base station.
- Sensor nodes can revise the transmission power of wireless transmitter according to the distance [7].
- Cluster head perform data aggregation and BS receives compressed data.
- The lifespan of WSN is the total amount of time before the first sensor node runs out of power [6].

3. FEATURES OF SENSOR NETWORKS

3.1 Lifetime: In sensor network, sensor nodes have limited battery power, so the life time of sensor nodes is less. Lifetime is more important in some more critical applications. Although it is often assumed that the transmit power associated with packet transmission accounts for the sensing, signal processing and even hardware operation in standby mode consume a consistent amount of power as well. In some applications, extra power is needed for macro- scale actuation [5]. At the physical layer routing and channel access protocols could be benefit to exchange the information. Lower radio duty cycles and dynamic scaling can be beneficial at physical layer for energy consumption. The loss of the sensor nodes due to battery depletion should avoided by using energy-efficient routing.

3.2 Flexibility: Sensor networks are dynamic in nature they can adapt the changes in nodes density and topology. Sensor networks should be scalable. In surveillance applications, most nodes may remain quiescent as long as nothing interesting happens. However, they must be able to respond to special events that the network intends to study with some degree of granularity [5]. In a self-healing minefield, a number of sensing mines may sleep as long as none of their peers explodes, but need to quickly become operational in the case of an enemy attack. In control application, respond time is very critical (sensor/actuator networks) in which the network is to provide a delay-guaranteed service [5]. In sensor network nodes are self-configure and nodes can easily adopt the different conditions. In sensor network, failure of individual sensor node, the sensor network robust to change in their topology. Connectivity and coverage in sensor nodes always be guaranteed. Connectivity is achieved if each node is connected to base station direct or indirect. To check the coverage of the network, to measure the quality of services is provide by network in particular area. Complete coverage is particularly important for surveillance applications.

3.3 Maintenance: The maintenance in a sensor network is very important. The sensor network is updated complete or partial over the wireless channel. All sensor nodes should be updated, and the restrictions on the size of the new code should be the same as in the case of wired programming. Packet loss must be accounted for and should not impede correct reprogramming [5]. The code which is always running in the nodes, should supported to reprogramming like a small footprint, and updating procedures should only cause a brief interruption of the normal operation of the node [5]. The failures can occur due to many reasons like battery depletion to unpredictable external events, may either be independent or spatially correlated. Fault-tolerance is particularly crucial as ongoing maintenance is rarely an option in sensor network applications. Self-configuring nodes should allow to deployment process run smoothly without human interaction, the nodes are placed in given specific geographical area. The nodes should be able to assess the quality of the network deployment and indicate any problems that may arise, as well as adjust to changing environmental conditions by automatic recon-figuration [5]. Time synchronous is must to cooperating among nodes, such as data fusion, channel access, coordination of sleep modi, or security-related interaction.

3.4 Data Collection: Data collection is related to network connectivity and coverage. An interesting solution is the use of ubiquitous mobile agents that randomly move around to gather data

ISSN 2348 – 7968

bridging sensor nodes and access points, it is often the case that all data are relayed to a base station, but this form of centralized data collection may shorten network lifetime [5]. Relaying data to a data sink causes non-uniform power consumption patterns that may overburden forwarding nodes. This is particularly harsh on nodes providing end links to base stations, which may end up relaying traffic coming from all other nodes, thus forming a critical bottleneck for network throughput. In sensor network we can use clustering technique to transmit information. The cluster nodes transmit the data or information to cluster head. Cluster head forward the data to a sink. Cluster nodes team up the cluster, in a cluster one node is cluster head and rest are the member of the cluster. Fewer packets are transmitted, and a uniform energy consumption pattern may be achieved by periodic re- clustering. Data redundancy is minimized, as the aggregation process fuses strongly correlated measurements [5]. In many applications some queries are needed that are sent to sensing nodes. For example, our goal is gathering a specific data or information regarding to a specific area, where many sensor nodes have been deployed. This is the rationale behind looking at a sensor network as a database. In a sensor network sensor nodes are able to protect its data and node itself from external nodes, but the severe limitations of lower-end sensor node hardware make security a true challenge.

4. ATTACKS IN WIRELESS SENSOR NETWORKS

Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, and so on. Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms).

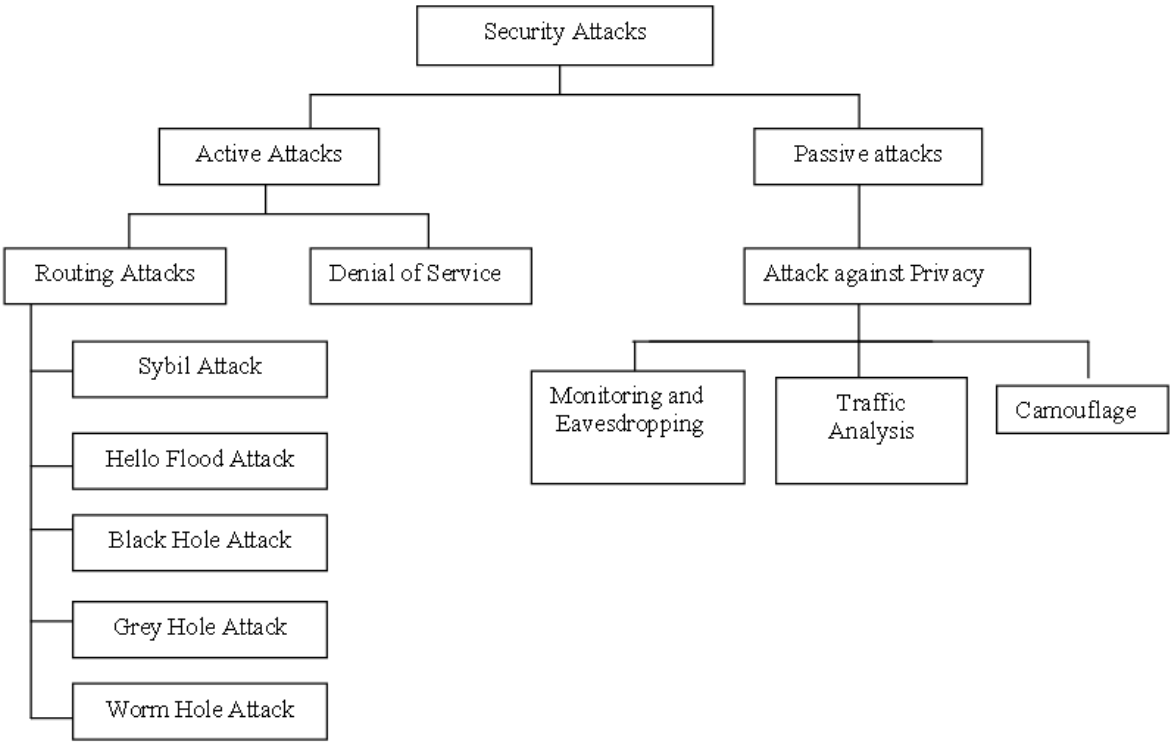

Figure 1.1: Different types of attacks in Wireless Sensor Networks

4.1 Active Attacks: The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The various attacks are active in nature like Denial of

ISSN 2348 – 7968

Service Attacks, Node Subversion, Node Malfunction, Node Outage, Physical Attacks, Message Corruption, False Node, Node Replication Attacks, and Passive Information Gathering etc.

4.1.1 Denial of Service: Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion and unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.[2]

4.1.2 Sybil attack: Newsome et al. describe the Sybil attack as it relates to wireless sensor networks. Simply put, the Sybil attack is defined as a "malicious de-vice illegitimately taking on multiple identities". It was originally de-scribed as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation and foiling misbehavior detection. Regardless of the target (voting, routing, ag-gregation), the Sybil algorithm functions similarly. All of the techniques involve utilizing multiple identities. For instance, in a sensor network voting scheme, the Sybil attack might utilize multiple identities to generate addi-tional "votes." Similarly, to attack the routing protocol, the Sybil attack
would rely on a malicious node taking on the identity of multiple nodes, and thus routing multiple paths through a single malicious node.

4.1.3 Hello Flood Attack: Most protocols require nodes to broadcast HELLO PACKETS to show their presence to their neighbours and the receiving nodes may assume that it is within the RF range of the sender. This assumption may prove to be false when a laptop-class attacker transmit routing information with an abnormally high transmission power to prove every other node in the network that the malicious node is its neighbour. Such an attack in the network is called a hello flood attack.

4.1.4 Black hole Attack: A black hole is a malicious node that attracts all the traffic in the network by advertising that it has the shortest path in the network [9]. So, it creates a metaphorical black hole with the malicious node or the adversary at the center. This black hole drops all the packets it receives from the other nodes. In a black hole attack, malicious nodes do not send true control messages. To execute a black hole attack, malicious node awaits the neighboring nodes to send RREQ messages.

4.1.5 Grey hole Attack: A grey hole attack is a variation of black hole attack in which the nodes selectively drops packets [1]. There are two ways in which a node can drop packets:
- It can drop all UDP packet s while transmitting all TCP packets.
- It can drop 50% of the packets or can drop them with probabilistic distribution.

In a grey hole attack a normal node can prevent from behaving usually and therefore this attack is difficult to detect. A grey hole attack affects one or two nodes in the network whereas a black hole attack affects the whole network.

4.1.6 Wormholes Attacks: In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them to another location, and retransmits them into the network. n the wormhole attack [1], an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convince nodes who would

normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the adversary on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive.

4.2 Passive Attacks: The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature.

4.2.1 Attacks against Privacy: The main privacy problem is not that sensor networks enable the collection of information. In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, sensor networks intensify the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information at low-risk in anonymous manner. Some of the more common attacks[8] against sensor privacy are:

- **Monitor and Eavesdropping:** This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection.
- **Eavesdropping attack:** Eavesdropping is the process of gathering information from a network by snooping on transmitted data and to eavesdrop is to secretly overhear a private conversation over a confidential communication in an unauthorized way. The information remains the same but its privacy is compromised. An attacker eavesdrops secretly between any two nodes and may collect the necessary information regarding connection such as MAC address and cryptographic information. An attacker may also steal the User Id and password information. Although this attack can be classified into other categories such as privacy-related attacks, we group it into this category since its consequences are severe in the sense that the collected cryptographic information may break the encryption keys such that the attacker can retrieve meaningful data. An example of eavesdropping is intercepting credit card numbers, using devices that interrupt wireless broadcast communications or tapping wire communication
- **Traffic Analysis:** Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network.
- **Camouflage Adversaries:** One can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

5. CHALLENGES IN WIRELESS SENSOR NETWORKS:

The sensor networks have a many technical challenges due to some factors as given:

- **Ad hoc deployment**: Most of sensor nodes are deployed in regions which have no infrastructure at all. A typical way of deployment in a forest would be tossing the sensor nodes from an aeroplane. In such a situation, it is up to the nodes to identify its connectivity and distribution [1].
- **Unattended operation:** In sensor network once the sensor nodes are deployed without human interaction this type of sensor network can easily reconfigure itself and adopt the changes in environment, if any changes are occur.
- **Untethered**: In a sensor network, the sensor nodes are not connected to any energy source. There is only a finite source of energy to sensor nodes, which must be optimally

ISSN 2348 – 7968

used for processing and communication like battery power. An interesting fact is that communication dominates processing in energy consumption. Thus, in order to make optimal use of energy, communication should be minimized as much as possible [2].

- **Dynamic changes**: Sensor network is dynamic in nature. The sensor nodes are configurable itself. Sensor nodes are easily adopting the changes in the sensor network due to addition of more sensor nodes in the network and failure of any node.
- **Fault tolerance:** The fault tolerance means to maintain the infrastructure in a form that if one node dies then it cannot affect the other nodes. The adaptive protocols are developed to maintain the other network unaffected.
- **Security issues:** Most of the threats and attacks against security in wireless networks are almost similar to their wired counterparts while some are exacerbated with the inclusion of wireless connectivity. In fact, wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping. In most of the cases various security issues and threats related to those we consider for wireless ad hoc networks are also applicable for wireless sensor networks.
- **Synchronization and Localization:** In some applications the data acquired in all nodes makes sense as a whole and therefore needs to be synchronized. Clock synchronization is an important service in sensor networks. Time Synchronization in a sensor network aims to provide a common timescale for local clocks of nodes in the network. . A global clock in a sensor system will help process and analyze the data correctly and predict future system behavior. This is not as trivial as it could appear because there are delays in transmission and there is no broadcasting clock to synchronize nodes. This is a major challenge in WSN.
  The localization of sensor nodes using just the relative positions of the sensors is also a major challenge in sensor networks. This is very important and researched area in which many approaches have been made such as exploiting received signal strength indicators, time of arrival, time difference of arrival, or angle of arrival. Distributed algorithms are playing a great role in increasing precision.
- **Short Range Transmission:** In wireless sensor networks we have to consider the short Transmission range in order to reduce the possibility of being eavesdropped. As in long in order to reduce the possibility of being eavesdropped. As in long range transmission we need high transmission power due to the point to point transmission between the nodes to reach the destination which increases the chance of being eavesdropped.
- **Energy consumption:** The energy consumption is a major challenge in WSN. As the sensor nodes are small in size and equipped with a limited number of power source. The sensor nodes are dependent on the battery which is very difficult to replace due to the physical constraints. Due to this reason many of researchers are focusing on the design of power aware protocols and algorithms. As the low- cost deployment is one acclaimed advantage of sensor network. Limited processor bandwidth and small memory are two arguable constraints in sensor networks, which will disappear with the development of fabrication techniques. However, the energy constraint is unlikely to be solved soon due to slow progress in developing battery capacity. The untended nature of sensor nodes and hazardous sensing environments preclude battery replacement as a feasible solution. On the other hand the surveillance nature of many sensor network applications requires along lifetime, it is a very important research issue to provide a form of energy efficient surveillance service for a geographic area.

6. CONCLUSION

ISSN 2348 – 7968

Wireless Sensor Networks are vulnerable to many types of attacks due to deployment of sensor nodes in an unattended environment. In this paper, we present a brief survey on wireless sensor network, its characteristics and challenges. There are two types of attacks in wireless sensor networks: Active and Passive attacks. As a infrastructure less network both types of attacks arise frequently, so our research focus is to create an automatic system that will detect and isolate the malicious nodes

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, Wireless sensor networks: A survey, Computer Networks, pp. 393-422, 2000.
[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine , 40(8):102–114, August 2002.
[3] H. Chan and A. Perrig. Security and privacy in sensor networks. IEEE Com-puter Magazine , pages 103–105, 2003 2003.
[4] A. Perrig, J. Stankovic, and D. Wagner. Security in wireless sensor networks. Commun. ACM , 47(6):53–57, 2004.
[5] Y. Xi, L. Schwiebert, and W. Shi. Preserving privacy in monitoring-based wireless sensor networks. In Proceedings of the 2nd International Workshop on Security in Systems and Networks (SSN ’06), . IEEE Computer Society, 2006.
[6] A.S.K. Pathan, H.W. Lee, C.S. Hong, Security in Wireless Sensor Networks: Issues and Challenges, Communications, IEEE Transaction, Feb 2006.
[7] J. Cai, P. Yi, J. Chen, Z. Wang, N. Liu, An Adaptive Approach To Detecting Black And Gray Hole Attacks In Ad Hoc Network, 24th IEEE International Conference on Advanced Information Networking and Applications, 2010
[8] D. Virmani, A. Soni, N. Batra, Reliability Analysis to Overcome Black hole Attack in Wireless Sensor Networks, Proceedings of The International Conference on Computing, Informatics and Networks, 2014, pp.45-51.
[9] V.P. Singh, A.S. Anand, S. Jain, Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks, International Journal of Computer Applications, vol. 62, no.15, 2013.