Journal of Information Systems and Communication
ISSN: 0976-8742 & E-ISSN: 0976-8750, Volume 3, Issue 1, 2012, pp.-251-255.
Available online at http://www.bioinfo.in/contents.php?id=45

A REVIEW OF ATTACKS ON WIRELESS SENSOR NETWORKS

PREETI SHARMA

Department of Computer Science & Engineering, SBS College of Engineering & Technology, Ferozpur, India
*Corresponding Author: Email- research0407@gmail.com

Received: January 12, 2012; Accepted: February 15, 2012

Abstract- The wireless sensor network is an emerging technology. It has become popular as it has variant applications in real world such as for medical monitoring, homeland security, industrial automation and verity of military applications. Sensor network provides endless opportunities but at same time pose various challenges as there are resource constraints like energy i.e. it has limited battery life, memory computation etc. The sensor network can also be used to monitor phenomena which discourage human presence. The sensor network deploy in hostile environment which increase the probability of being attack by adversary. The wireless communication technology also acquire various types of security threats, it is very important to understand the security challenges and issues in order to design appropriate security mechanisms. This paper will discuss about sensor networks, security requirements, various challenges and issues and attacks.
Keywords- wireless sensor networks, constraints, security challenges and issues, attacks

Citation: Preeti Sharma (2012) A Review of Attacks on Wireless Sensor Networks. Journal of Information Systems and Communication ISSN: 0976-8742 & E-ISSN: 0976-8750, Volume 3, Issue 1, pp.- 251-255.

Wireless Sensor Networks

A wireless sensor network is a network of spatially distributed sensor which use to monitor physical or environmental conditions like temperature, pressure, pollution contents in air, sound , vibration etc. in other words we can define it as a wireless sensor network is self configuring network of small sensor nodes which communicate with each other via radio signals and deployed in quantity to sense, monitor and understand the physical world.WSN combines sensing, computation and communication in a single device called sensor node A wireless sensor nodes are called motes. Sensor nodes have capability to collect sensed data and send that to the base station, a WSN generally consist of a base station that can communicate with a number of wireless sensors via radio link. Data is collected at the sensor node ,compressed and transmitted to the base station directly or if required use other sensor nodes to forward data to base station A sensor consist of four basic part a sensing unit, a processing unit, a transceiver unit and a power unit. a sensing unit is basically a senor ,processing unit is a microcontroller or a circuit chip to process data, transceiver is a radio transceiver with internal antenna or connection to external antenna and the power unit usually battery. Application of sensor networks are varied typically involving some kind of monitoring, tracking and controlling there are many sensor network applications like such environmental data collection, security monitoring, medical science, tracking. Energy is the scarcest resource of WSN node as it determines the lifetime of the WSN for these reason algorithms and protocols need to address the issues like - lifetime maximization, robustness, fault tolerance and self-configuration

Why Wireless Sensor Network

WSNs have attracted much attention due to its great potential to be used in various applications. Comparing to existing infrastructure - based networks, wireless sensor networks can virtually work in any environment, especially those where wired connections are not possible[1].Scientists develop wireless sensor networking on the bases of inspiration from the application known as battle field surveillance which is completely a military application. As we know that this technology has great importance in the field of computational world and where it has computational importance it also has importance in industry. It is also play an important part in civilian technologies like monitoring of traffic control and many others[2].

Wireless Sensor Network's Applications

In the present era there are lot of technologies which are used for monitoring are completely based on the wireless sensor networking. Some of important applications are environmental monitoring, traffic control application, weather checking, regularity checking of temperature etc. Wireless sensor networks can also be used for detecting the presence of vehicles such as motor cycles up to trains. These are some important wireless sensor networking based technologies which help us in our daily life. Some of their daily life applications are: used in agriculture, water level monitoring, green house monitoring, landfill monitoring[3] . Sound Surveillance System (SOSUS) is the first obvious sensor networks application. It had been used during the Cold War in the early 1950s to detect and track Soviet submarines with the help of acoustic sensors or hydrophones. The Distributed Sensor Networks (DSN) program was then initiated by the Defence Advanced Research Projects Agency (DARPA) around 1980[4].In the University of California at Berkeley and the College of the Atlantic, environmental monitoring is carried out off the coast of Maine on Great Duck Island by means of a network of Berkeley motes equipped with various sensor. The nodes send their data to a base station which makes them available on the Internet. Since habitat monitoring is rather sensitive to human presence, the deployment of a sensor network provides a non invasive approach and a remarkable degree of granularity in data acquisition .The same idea lies behind the Pods project at the University of Hawaii at Manoa , where environmental data (air temperature, light, wind, relative humidity and rainfall) are gathered by a network of weather sensors embedded in the communication units deployed in the South-West Rift Zone in Volcanoes National Park on the Big Island of Hawaii. Sensor networks can also be used to monitor and study natural phenomena which intrinsically discourage human presence, such as hurricanes and forest fires[5]..

Constraints In Wireless Sensor Network

A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks[6]. All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

Limited memory and storage space

A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm.

Power limitation

Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced or recharged. Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network.

Security Requirnment

The wireless sensor network have application in military areas for intrusion detection etc In that case sensor need to send data to base station or another sensor on wireless medium which is vulnerable to attacks. Each sensor node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical point of attack or logical attack. The network may be dispersed over a large areas , further exposing them to attackers who capture and reprogram individual sensor node attackers can also induce their own node as legitimate sensor node via node replication or they can claim multiple identities for an altered node, once in control of few nodes inside the network ,the adversary can then mount a variety of attacks- for example falsification of sensor data, extraction of private sensed data from sensor network reading and denial of service attack.
The security requirement in WSN includes:

- **Availability:** It ensures that desired network services are available even in the presence of denial of service attacks.
- **Authorization:** It ensures that only authorized sensors can be providing information to network services.
- **Authentication:** it ensures that the communication from one node to another node is genuine, that is a malicious node cannot masquerade as a trusted sensor node.
- **Confidentiality:** It ensures that a given message cannot be understood by anyone other than the desired recipients.
- **Integrity:** It ensures that a message sent from one node to another is not modified by malicious intermediate nodes.
- **Non repudiation:** It denotes that a node cannot deny sending a message it has previously sent.
- **Freshness:** it denotes that data is fresh means its recent and ensures that no adversary can replay old message

Security Challenges In Wireless Sensor Network

- The wireless sensor network using wireless medium inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Although this problem is not unique to sensor networks, traditional solutions must be adapted to efficiently execute on sensor networks [7].
- The extreme resource limitations of sensor devices pose considerable challenges to resource: hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory. This is no trivial task. Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of power. Clearly, security mechanisms must give special effort to be communication efficient in order to be energy efficient [7]. Higher security levels in WSNs usually correspond to more energy consumption for cryptographic functions.
- The ad-hoc nature of sensor networks means no structure can be statically defined. The network topology is always subject to changes. Nodes may be deployed by airdrop, so

nothing is known of the topology prior to deployment. Since nodes may fail or be replaced the network must support self-configuration. Security schemes must be able to operate within this dynamic environment

The proposed scale of sensor networks poses a significant challenge for security mechanisms. Providing security over such a network is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency

Security Issues In Wireless Sensor Network

The security issues can be categories as cryptography, key management, secure routing, secure data aggregation, intrusion detection. Selecting the most appropriate cryptographic method is vital in WSNs because all security services are ensured by cryptography. Cryptographic methods used in WSNs should meet the constraints of sensor nodes and be evaluated by code size, data size, processing time, and power consumption. Most of the traditional techniques, however, are unsuitable in low power devices such as wireless sensor networks. This is due largely to the fact that typical key exchange techniques use asymmetric cryptography, also called public key cryptography Symmetric schemes utilize a single shared key known only between the two communicating hosts. The constraints on computation and power consumption in sensor nodes limit the application of public key cryptography in WSNs. Thus, most research studies focus on symmetric key cryptography in sensor networks. Public key algorithms such as RSA are computationally intensive and usually execute thousands or even millions of multiplication instructions to perform a single security operation[8]. In contrast, symmetric key cryptography algorithms and hash functions consume much less computational energy than public key algorithms.

As for the security purpose cryptography is used. The cryptographic system such as those used symmetric key cryptography or public key mainly relies on secrecy of the keys it uses. If an attacker can find the key, the entire system is broken because the attacker can use the key to decrypt the intercepted ciphertexts to find the original plaintexts. Therefore sender and receiver required to update the keys between them time to time. In a WSN, some sensor nodes may be captured by an attacker; thus, the key information is accessible to the attacker and can be used to launch other serious attacks. Therefore, a very important issue is how to securely manage the keys between the sender and the receiver. The goal of networking is to provide an infrastructure for delivering data from a source node to a destination node. Routing protocols are the most critical component because they address the problem of how to find a path from the source to the destination and finally take charge of data delivery[9]. the routing protocol can be categorize as flat based routing , hierarchical based routing and location based routing. Next is secure data aggregation a key technique employed to optimize the energy resources in the sensor nodes; wherein the data sensed from different sensor nodes forming one group is collected and aggregated by an aggregator node and then, only a single packet is transmitted upstream, to either the base station or further aggregating nodes [10].by looking at the present scenarios only security mechanisms cannot ensure perfect security. Since sensor nodes can be compromised, it is easy for an adversary to inject false data into a WSN through the compromised nodes. Authentication and data encryption are not enough for ensuring data security. Another approach to protect WSNs involves mechanisms for detecting and reacting to intrusions.It requires intrusion detection system that will make decision based on some patterns. Ids will use that pattern to differentiate attacker node and legitimate node

Attacks In Wireless Sensor Networks

Wireless networks are more vulnerable to security attacks than wired networks, due to the broadcast nature of the transmission medium. These attacks are normally due to one or more vulnerabilities at the various layers in the network.[11] Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Attacks on sensor networks can be classified into attacks on its layers like physical, link, network, transportation, and application layers. Attacks can also be classified based on the capability of the attacker, such as sensor level and laptop-level. A powerful laptop-level adversary can do much more harm to a network than a malicious sensor node, since it has much better power supply, as well as larger computation and communication capabilities than a sensor node. Attacks can also be classified into outside and inside attacks. An outside attacker has no access to most cryptographic materials in sensor networks, while an inside attacker may have partial key materials and the trust of other sensor nodes. Inside attacks are much harder to detect and defend against[12].basically attacks can be classified as active attacks or passive attacks.

Passive Attacks

In passive attacks passive attacker only listens or monitors the communication channel passively and makes no modification to data pass through it. Some more common attacks are

- **Monitor and Eavesdropping**- This is the most obvious attack to privacy. By listening 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.
- **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[7].
- **Camouflage** Attacker can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can masquerade as a normal node to attract the packets, then misroute *the packets, e.g. forward the packets to the nodes conducting the privacy* analysis

Active Attacks

In active attacks attacker actively listen or monitors the communication channel so that he can make modification to the data pass through it, more common active attack is denial of service attack. [13]We consider any kind of attempt of an adversary to disrupt, subvert, or destroy the network as a denial of service attack. In practicality, a DoS situation can occur due to any kind of incident

that diminishes, eliminates, or hinders the normal activities of the network. Say for example, any kind of hardware failure, software bug, resource exhaustion, environmental condition, or any type of complicated interaction of these factors can create denial of service.

Layer based attacks

Physical layer

Responsible for frequency selection, carrier frequency generation, signal deflection, modulation and data encryption**.** Two types of attacks can be performed on this layer are jamming and tempering.

Jamming: Is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network. The jamming of a network can come in two forms: constant jamming, and intermittent jamming. Constant jamming involves the complete jamming of the entire network. No messages are able to be sent or received. If the jamming is only intermittent, then nodes are able to exchange messages periodically, but not consistently. Spread spectrum[14] communication is a common defence against physical-layer jamming in wireless networks. Unfortunately, low-power, low-cost sensor nodes are usually limited to simple radios that can't use these techniques. If WSN nodes can identify a jamming attack, a logical defence is to put sensors into a long-term sleep mode and have them wake periodically to test the channel for continued jamming.

Tampering: An attacker can physically damage or replace sensor and computation hardware or extract sensitive information such as cryptographic keys to gain unrestricted access to higher levels of communication. Defense against clever passersby and corrupt insiders is easier and cheaper than defense against well-funded governments. [15]When possible, the node should react to tampering in a fail-complete manner. It could, for example, erase cryptographic or program memory. Other traditional physical defences include camouflaging or hiding nodes.

Data link layer

Responsible for multiplexing of data stream, data frame detection, medium access and error control**.** Possible attacks at this layer are collision and exhaustion.

Collision: A collision occurs when two nodes attempt to transmit on the same frequency simultaneously. When packets collide, a change will likely occur in the data portion, causing a checksum mismatch at the receiving end. Such collisions would require the retransmission of any packet affected by the collision. Using this technique it would be possible for an attacker to simply deplete a sensor node's power supply by forcing too many retransmissions. The network [14]can use collision detection to identify these malicious collisions, which create a kind of link-layer jamming, but no completely effective defence is known. Proper transmission still requires cooperation among nodes, which are expected to avoid corruption of others' packets.

Exhaustion: Repeated collisions can also be used by an attacker to cause resource exhaustion. one solution to it could be the use of time division multiplexing. Another possible solution is to apply rate limits to the MAC admission control.

Network layer

Responsible for specifying the assignment of addresses and how packets are forwarded**.** Possible attacks could be

Spoofed, altered, or replayed routing information: The most direct attack against a routing protocol is to target the routing information exchanged between nodes. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency[16].

Sinkhole: 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 [17].

Sybil attack: the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, 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[18]. To detect the Sybil attack, two methods can be used One method is radio resource testing in which each node assigns a unique channel to each of its neighbours, including fake neighbours, and tests whether its neighbors can communicate with it through the assigned channels. Because the radio of a sensor platform is usually incapable of simultaneously sending or receiving on more than one channel, the failure of communication through one channel may be a sign of the Sybil attack[9].

Selective forwarding attack: In selective forwarding attack a malicious node may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further [19]. A [20] special form of this attack known as black hole attack. Two different countermeasures have been proposed against selective forwarding attack. One defence is to send data using multi path routing. Another one is detection of compromised nodes which are misbehaving in terms of selective forwarding and route. the data seeking an alternative path.

Wormhole attack: An adversary can tunnel messages received in one part of the network over a low latency link and replay them in another part of the network. The simplest[21] instance of this attack is a single node situated between two other nodes forwarding messages between the two of them.

Hello flood attack: We introduce a novel attack against sensor networks: the HELLO flood. 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 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 neighbour[22]**.**

Transport layer
responsible for specifying how reliable transport of packets will take place
Flooding: Aattacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored.

Other types of attacks could be
Node subversion: The wireless sensor network deployed in hostile environment which increase the probability of capturing of a node or we can say a node can be physically attack by adversary and important material like cryptographic keys can be fetched. A particular sensor might be captured, and information (key) stored on it might be obtained by an adversary.
Node malfunction: A malfunctioning node will generate inaccurate data that could expose the integrity of sensor network especially if it is a data-aggregating node such as a cluster leader.
Node outage: in node outage node stops its function in case where a cluster head stops functioning the sensor network protocols should be able to mitigate the effects of node outage by providing an alternate route.

Conclusion
As we discussed how security become important in wireless sensor networks. Security in sensor networks has attracted many researchers as it become important to work on it. This paper mainly concentrated on various security challenges, issues and different types of attacks. This review could help future researchers to come up with smarter & better security mechanisms / solutions and make their network safer.

References

[1] Zorans Bojkovic., Bojan Bakmaz M. and Miodrag R. Bakmaz (2008) *Journal of communications* 2(1).
[2] *www.wifinotes.com/how-wireless-sensor-networks-works.html*.
[3] Haenggi M. Ilyas M. and Mahgoub I. eds., Boca Raton (2004) *Compact Wireless and Wired Sensing Systems*, 1.1-1.14.
[4] Khemapech ducan and Miller A., *A survey of wireless sensor networks technology*.
[5] Daniele Puccinelli and Martin Haenggi, *wireless sensor network: applications and challenges of ubiquitous sensing*.
[6] John paul walters, zhengqiang liang, weisong shi and Vipin Chaudhary (2006) *wireless sensor networks security: a survey" security in distributed, grid and pervasive computing*.
[7] Padmavathi G., Shanmugapriya D. (2009) *Journal of Computer Science and Information*, 4, 1-2.
[8] Yong Wang, Garshan Atterbury and Byrav Ramamurthy (2006) *IEEE communications surveys* 2*nd quarter*, 8(2).
[9] Yun Zhou and Yuguang Fang, Yanchao Zhang (2008) *IEEE communications* 3*rd quarter* 10(3).
[10] Jinwala D.C., Dhiren R. Patel, Dasgupta K.S. *A survey of security issues in wireless sensor networks*.
[11] Shio kumar Singh, Singh M.P. and Singh D.K. (2011) *International journal of computer trends and technology.*
[12] Xiaojang du, Msiao- hwa chen (2008) *IEEE wireless communications* .
[13] [Jal-sakib khan Pathan, *communications and media research*.
[14] David R. Raymond and Scott F. Midkiff *IEEEcs Temparing*.
[15] Anthony D. Wood, John A. Stankovic (2002) *Denial of service in sensor networks, IEEE*.
[16] Karlof C. and Wagner D., *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures*, *First IEEE Int'l*.
[17] Ritu Sharma, Yogish Chaba, Yudhvir Singh, *Int j Advance networking and applications,* 2(3).
[18] Al sakib khan pathan, hyung-woolee choong seon hong (2006) *ICACT*.
[19] Prabhudutta Mohanty, Sangram Panigrahi, Nityananda Sarma and Sidhartha Sanker Satapathy, *journal of theoretical and applied information technology*.
[20] Jihan Rehana *TKKT\- Seminar on inter networking* 110.5190
[21] Snehlata Yadav, Kamlesh Gupta and Sanjay Silakari (2010) *journal of information systems and communication*,1(2).
[22] Chris karlof, David Wagner *Secure routing in wireless sensor network : attacks and countermeasure*.