Volume: 04 Issue: 04 Pages:1657-1661 (2013) ISSN : 0975-0290

Security Threats in Wireless Sensor Networks in Each Layer

Anitha S Sastry
Email : anithasastry@gmail.com
Department of Electronics and Communication Engineering, Global Academy of Technology, Bangalore-98
Shazia Sulthana
Email : shaziasulthana@yahoo.co.in
Department of Electronics and Communication Engineering, Global Academy of Technology, Bangalore-98
Dr. S Vagdevi
Department of Information Science and Engineering, Global Academy of Technology, Bangalore-98
Email: dr.vagdevi@gat.ac.in

----------ABSTRACT----------

As the Wireless Sensor Networks (WSN) prove to be more beneficial in real-world applications. At the same time threatened by vulnerabilities. The threats faced by these WSN are similar but not limited to those observed in a simple network of computers or Internet. Attacks at all the layers of network protocol can be expected. Wireless sensor networks are characterized by severely constrained computational and energy resources and ad hoc operational environment. Resource limitations of WSN make these threats even more dangerous, even up to the extent of the consumption of a whole node or even a complete small network. This paper deals with the security aspects in the wireless sensor network giving the probable counter measures for the same.

Keywords – **Data Authenticity, WSN, Attacks on sensor networks, Denial of Service, Reliability, Availability**

Date of Submission: November 25, 2012 Date of Acceptance: January 21, 2013

I. INTRODUCTION

Every network, whether internet or an ad hoc wireless network, is vulnerable to malicious activity. The Wireless Sensor Networks are no less vulnerable. The attacks on WSN prove to be even more destructive than those on internet or other ad hoc networks. The reason is the WSN consists of nodes with very limited resources whereas the attacker may have very powerful attacking (malicious) resources such as laptops with wireless LAN capability, long range wireless communication capability etc. Therefore security in WSN is a major issue. The security techniques of the normal computer networks cannot be implemented in WSN because of limited resources. Considering, for example, the asymmetric cryptographic algorithm (such as RSA with 1024 bits) the memory of a typical sensor node is not sufficient enough to hold even the variables for its implementation. Even if memory is allowed the computation time would be enormous. To worsen the situation the power available with a sensor node is also very small (and the node may entirely consume even in a single computation). So we may conclude that the normal computationally heavy algorithms of security can't be applied on the *weak (*resource limited) *WSN*. An inevitable requirement of security and integrity of the WSN network is required as well as it exists in the internet or the other wireless ad hoc networks. Otherwise, without incorporating security feature, a sensor network may never be able to serve us to do our needs full. [1]

A holistic approach aims at improving the performance of wireless sensor networks with respect to security, longevity and connectivity under changing environmental conditions. The holistic approach of security concerns about involving all the layers for ensuring overall security in a network. For such a network, a single security solution for a single layer might not be an efficient solution rather employing a holistic approach could be the best option.

The holistic approach has some basic principles like, in a given network; security is to be ensured for all the layers of the protocol stack, the cost for ensuring security should not surpass the assessed security risk at a specific time, if there is no physical security ensured for the sensors, the security measures must be able to exhibit a graceful degradation if some of the sensors in the network are compromised, out of order or captured by the enemy and the security measures should be developed to work in a decentralized fashion. If security is not considered for all of the security layers, for example; if a sensor is somehow captured or jammed in the physical layer, the security for the overall network breaks despite the fact that, there are some efficient security mechanisms working in other layers. By building security layers as in the holistic approach, protection could be established for the overall network.

The paper is organized as follows. Section II describes security classes. Section III describes about different threats in sensor network layers with probable countermeasures.

Volume: 04 Issue: 04 Pages:1657-1661 (2013) ISSN : 0975-0290

II. SECURITY CLASSES

- Attacks on wireless network can be broadly classified as interruption, interception, modification and fabrication.
- Interception is an attack on confidentiality. The sensor network can be compromised by an adversary to gain unauthorised access to sensor node or data stored within it.
- Modification is an attack on integrity. Modification means an unauthorised party not only accesses the data but tampers it, for example by modifying the data packets being transmitted.
- Fabrication is an attack on authentication. In fabrication, an adversary injects false data and compromises the trustworthiness of the information relayed.

Network Security Threats

Different threats at each layer in OSI model can be summarized as in table I.

Table.1

Layers	Attacks
Physical layer	Jamming, Tampering
Data link layer	Jamming, Collision
Network layer	Spoofing or replaying information, Selective forwarding or black holes, Sink holes, Sybil attacks, Node replication attacks, Wormholes Flooding, Attacks against privacy
Transport layer	Injects false messages , Energy drain attacks
Application layer	Attacks on reliability

III. SENSOR NETWORK SECURITY IN PHYSICAL LAYER

The objective of physical layer is to increase the reliability by reducing path loss effect and shadowing. This layer is responsible for established connection, data rate, modulation, data encryption, signal detection, frequency generation and signal detection.

The most common attacks on the physical layer are jamming and tampering.

A. Jamming

The radio signal transmission can interfere with the radio frequencies used by the WSN, which is called jamming. As the adversary capability increases, it can affect larger portions of the network by sending other radio signals. The adversary can use few nodes to block the entire network. This condition is called jamming at the physical layer and hence resulting in denial-of-service. In this situation the adversary will not be able to get any data but will be able to block some nodes.

B. Tampering

Sometimes the nodes are physically tampered by an adversary. Such condition is called tampering. A tampering attacker may damage, replace, and electronically interrogate the nodes to acquire information [10]. Strong counter-measures against jamming have been designed like spread-spectrum, and frequency-hopping [1]

IV. SENSOR NETWORK SECURITY ISSUES AT DATA LINK LAYER

The objective of Data link layer is to insure interoperability amongst communication between nodes to nodes. This layer is responsible for error detection, multiplexing, prevention of collision of packets, repeated transmission etc.

The data link layer is vulnerable due to the reason that the data is transmitted in an open insecure medium. Hence it is susceptible to the attacks on the authenticity, integrity and confidentiality of the data being routed [1]. The main attacks at data link layer are collision and jamming.

A. Collision: For WSNs the transfer of a data packet may fail if the radio channel was currently occupied by another sensor node. This results in occurrence of too many collisions on the radio channel. Therefore, we cannot afford to establish a resource demanding communication between a base station and the sensor nodes. Collisions can be avoided with the distinct time slot assignment to each sensor node.

B. Jamming: Jamming can occur when the data get jammed with radio signals from other transmissions.

V. SENSOR NETWORK SECURITY ISSUES AT NETWORK LAYER

The objective of Network layer is to find best path for efficient routing mechanism. This layer is responsible for routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa. Vulnerabilities at network layer are,

- Spoofing or replaying information
- Selective forwarding or black holes
- Sink holes
- Sybil attacks
- Node replication attack
- Wormholes
- Flooding
- Attacks against privacy

A. Spoofing

A spoofing attack is a situation in which one person or program successfully disguises as another by falsifying data and thereby gaining an illegitimate advantage. Through spoofing, or replaying the routed information the network traffic can be extensively corrupted. Continuous alterations in messages which result in the packet loss during transmission may require the individual nodes to

Volume: 04 Issue: 04 Pages:1657-1661 (2013) ISSN : 0975-0290

retransmit packets continually. Thus the nodes may become dead much earlier than their expected life due to power exhaustion. Similarly sometimes replaying messages results in creating huge amount of traffic flow on the network. E.g. there may be a small broadcast message on the network, and some malicious node may capture this message and replay, hence damaging the network performance as shown in figure 1.

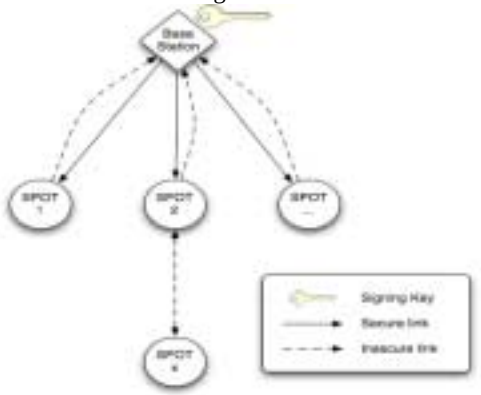

Fig.1: Spoofed attack

B. Selective forwarding or black holes

Normally the sensor networks are multi-hop systems. So, the sensors pass information from one end to the base station by routing them through intermediate nodes. Sometimes a malicious node may be present within the network path. In a flooding based protocol, the attacker (malicious node) listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. [9] Then the target may choose the route which contains the malicious node. This malicious node present in the route may selectively forward the data packets, i.e. forwards some packets to the next node, and drops others. The result is loss of huge amount of data, during the multi-hop information exchange process. In another case it may happen that the malicious node drops all the packets it receives, hence no information is forwarded. This creates a *black hole*. Such attacks are effective when the attacker is explicitly included in the data path of sensor network.

C. Sinkholes

In this attack the attacker lures most of the sensor network traffic to pass through the malicious node thus creating a sinkhole with malicious node at its center . Since now most of the data is being routed through the malicious node, the attacker/malicious node can play anything with the sensor data. [5] Many other attacks such as wormhole, selective forwarding or eavesdropping can be initiated through this sinkhole attack. The Fig 8 demonstrates sinkhole attack where 'SH' is a sinkhole. This sinkhole attracts traffic from nearly all the nodes to rout through it.

D. Sybil Attacks

In many cases, 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 Sybil attack [6], the attacker/malicious node show multiple identities. Since each actual node in a sensor network has a single identity, hence numerous threats can be observed. Since adversary has multiple identities, the innocent nodes may be routing multi-path data through the same malicious node [1] as shown in figure 2.

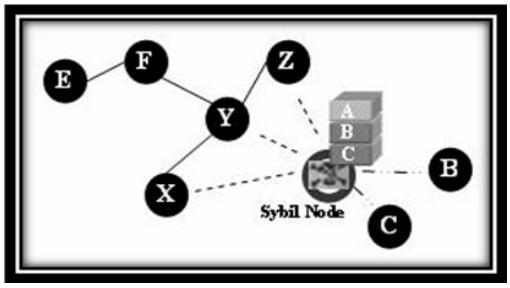

Fig. 2: Sybil Attack

Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection. Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to Sybil attack. However, as WSNs can have some sort of base stations or gateways, this attack could be prevented using efficient protocols. Detection of Sybil nodes in a network is not so easy. Newsome et. al. used radio resource testing to detect the presence of Sybil node(s) in sensor network and showed that the probability to detect the existence of a Sybil node is:

$$P_r\left(detection\right) = 1 - \left(1 - \sum_{allS,M,G} \frac{\binom{s}{S}\binom{m}{M}\binom{g}{G}}{\binom{n}{c}} \frac{S-(m-M)}{c}\right)^r \quad -(1)$$

Where, n is the number of nodes in a neighbor set, s is the number of Sybil nodes, m malicious nodes, g number of good nodes, c is the number of nodes that can be tested at a time by a node, of which S are Sybil nodes, M are malicious (faulty) nodes, G are good (correct) nodes and r is the number of rounds to iterate the test [9].

Countermeasures: Using a globally shared key allows an insider to masquerade as any (possibly even nonexistent) node. Identities must be verified. This attack can be avoided if we centrally compute the data gathering path by the BS then multiple place occurrence of the node can be detected. The other way to detect the attack is verifying the identities (authentication) of nodes by a trustworthy node.

F. Wormholes

Two malicious nodes may create a hidden channel (route) between them [8]. This is known as wormhole attack. The two malicious nodes may be communicating over very powerful data link as compared to the link between the actual sensor nodes. In this case also there many possibilities of attacks [1]. The two malicious nodes may be present in different locations in the network, and the attacker records the packets (or bits) at one location in the

Volume: 04 Issue: 04 Pages:1657-1661 (2013) ISSN : 0975-0290

network and tunnels those to another location. The tunneling or retransmitting of bits could be done selectively [9]. In another case the attackers may create a sinkhole by attracting their neighbor nodes for optimal routing to the base station. This can happen when the geographic routing is employed.

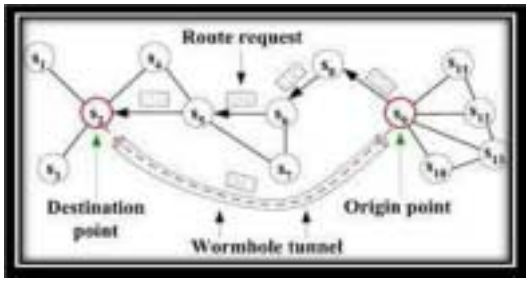

Fig. 3: Wormhole Attack

Figure 3 shows a situation where a wormhole attack takes place. When a node S_2 (for example, the base station or any other sensor) broadcasts the routing request packet, the attacker receives this packet and replays it in its neighborhood. Each neighboring node receiving this replayed packet will consider itself to be in the range of Node S_2, and will mark this node as its parent. Hence, even if the victim nodes are multihop apart from B, attacker in this case convinces them that S_2 is only a single hop away from them, thus creates a wormhole.

Countermeasures for Sink Holes and Worm Hole Attack:
Wormhole and sinkhole attacks are very difficult to defend against, especially when the two are used in combination. Wormholes are hard to detect because they use a private, out-of-band channel invisible to the underlying sensor network. Sinkholes are difficult to defend against protocols that use advertised information as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify. Routes that minimize the hop-count to a base station are easier to verify, however hop count can be completely misrepresented through a wormhole. The best solution is to carefully design routing protocols which avoid routing race conditions and make these attacks less meaningful. For example, one class of protocols resistant to these attacks is geographic routing protocols. A wormhole is most effective when used to create sinkholes or artificial links that attract traffic. Artificial links are easily detected in geographic routing protocols because the ‘‘neighboring’’ nodes will notice the distance between them is well beyond normal radio range.

G. Flooding
Sometimes the malicious node can cause immense traffic of useless messages on the network. This is known as the flooding. Some, times malicious nodes replay some actual broadcast messages, and hence generating useless traffic on the network. This can cause congestion, and may eventually lead to the exhaustion of complete nodes. This is a form of Denial of Service attack [1].

Countermeasures: The simplest defense against HELLO flood attacks is to verify the bi directionality of a link before taking meaningful action based on a message received over that link. However, this countermeasure is less effective when an adversary has a highly sensitive receiver as well as a powerful transmitter. One possible solution to this problem is for every node to authenticate each of its neighbors with an identity verification protocol using a trusted base station. If the protocol sends messages in both directions over the link between the nodes, HELLO floods are prevented when the adversary only has a powerful transmitter because the protocol verifies the bidirectionality of the link. Although this does not prevent a compromised node with a sensitive receiver and a powerful transmitter from authenticating itself to a large number of nodes in the network, an observant base station may be able to detect a HELLO flood is imminent.

VI. SENSOR NETWORK SECURITY ISSUE AT TRANSPORT LAYER

The objective of Transport Layer is to establish communication for external networks i.e. Sensor network connected to the internet. This is most challenging issue in wireless sensor networks. Sometimes the attacker might be strong enough to reach up to the transport layer, due to the attack being undetected at the lower layers. Transport layer attacks are injection of false messages and energy drain attacks [11] and are classified as follows:

A. Data integrity attack
Data integrity attacks compromise the data travelling among the nodes in WSN by changing the data contained within the packets or injecting false data. The attacker node must have more processing, memory and energy than the sensor nodes. The goals of this attack are to falsify sensor data and by doing so compromise the victim’s research. It also falsifies routing data in order to disrupt the sensor network’s normal operation, possibly making it useless. This is considered to be a type of denial of service attack. This attack can be defended by adapting asymmetric key system that is used for encryption or we can use digital signatures, but this requires a lot of additional overhead.

B. Energy drain attack
WSN is battery powered and dynamically organized. It is difficult or impossible to replace/recharge sensor node batteries. Because there is a limited amount of energy available, attackers may use compromised nodes to inject fabricated reports into the network or generate large amount of traffic in the network. Fabricated reports will cause false alarms that waste real world response efforts, and drain the finite amount of energy in a battery powered network. However the attack is possible only if the intruder’s node has enough energy to transmit packets at a constant rate. The aim of this attack is to destroy the sensor nodes in the network, degrade performance of the network and ultimately split the network grid and consequently take control of part of the sensor network by inserting a new Sink node [11]. To minimize the damage caused by this

Volume: 04 Issue: 04 Pages:1657-1661 (2013) ISSN : 0975-0290

attack fabricated reports should be dropped en-route as early as possible.

VII. SENSOR NETWORK SECURITY ISSUE AT APPLICATION LAYER

The objective of Application Layer is to present final output by ensuring smooth information flow to lower layers. This layer is responsible for data collection, management and processing of the data through the application software for getting reliable results.

Main attack at application layer is attacks on reliability

A. Attacks on reliability:

If an adversary changes the data in one path then it puts a question mark on the reliability of the data. In this attack attacker needs to identify the path of communication and put adversary in that path to change the data. An adversary can generate false data or query by joining the network. When a node responds to these wrong data or query, leads them to suffer from the energy drain attack. Usually to ensure reliability acknowledgement is expected for each successful data delivery [11].

VIII. CONCLUSION

In this paper a survey of various threats expected at each layer of the sensor networks. Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. Again, ensuring holistic security in wireless sensor network is a major research issue. Many of today's proposed security schemes are based on specific network models. Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against mote-class attackers, but cryptography alone is not enough. As there is a lack of combined effort to take a common model to ensure security for each layer, in future though the security mechanisms become well-established for each individual layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge.

REFERENCES

[1]. Asif Habib "Sensor Network Security Issues at Network Layer " *2nd International Conference on Advaificances in Space Technologies, Pp.* 58 - 63 *National Engineering and Scientific Commission, Islamabad, Pakistan.*.

[2]. A. Lapidoth and P. Narayan. "Reliable communication under channeluncertainty". *IEEE Transactions on Information Theory, 44(6), 1998.*

[3]. Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victorwen and David E. Culler, "SPINS: Security Protocols for Sensor Networks", Wireless Networks vol.8 Pp.521-534,2002.

[4]. C. Karlof, D. Wagnor, "Secure routing in wireless sensor networks: attacks and countermeasures", Ad Hoc Networks 1,Pp.293–315,2003.

[5]. Haowen Chan, and Adrian Perrig, "Security and Privacy in Sensor Networks" *Carnegie Mellon University pp. 99-101*.

[6]. John R. Douceur, "The Sybil attack", *Microsoft Research, 2002.*

[7]. 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, May 2005.*

[8]. Yih-Chun Hu, Adrian Perrig, and David B. Johnson. "Packet leashes: A defense against in wireless networks". *In Proceedings of IEEE Infoc wormhole attacks om April 2003.*

[9]. Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", *International Conference on Advaificances in Space Technologies.*

[10]. Shahnaz Saleem1, Sana Ullah2, Hyeong Seon Yoo1 "On the Security Issues in Wireless Body Area Networks" *International Journal of Digital Content Technology and its Applications Volume 3, Number 3, September 2009*

[11]. Prabhudutta mohanty, Sangram Panigrahi, Nityananda sarma and siddhartha sankar satapathy "Security issues in wireless sensor network data gathering protocols: a survey" *Journal of Theoretical and Applied Information Technology* .

Authors Biography

Anitha S Sastry is a Assistant Professor in the department of Electronics and Communication Engineering, Global Academy of Technology, Bangalore. She obtained her B.E. Degree in Electronics and Communication from Visvesvaraya Technological University, Bangalore. Her specialization in Master degree was Electronics from Visvesvaraya Technological University, Belgaum. She is pursuing research in the area of Security Issues in Wireless Sensor Networks. Her area of interest is in the field of Security in Communication Networks. He is life member of KRVP, Bangalore.

Dr. S Vagdevi is a Professor and Head, Dept. of Information Science and Engineering, Global Academy of Technology, Bangalore. She acquired Bachelor in Electrical Engineering and Masters in Power Systems from Bangalore University. She also has a Masters in Software systems from BITS, Pilani. She was awarded a P.D in Computer Science and Engineering from Vinayaka Mission University(VMU), Tamil Nadu.

.