SECURITY CONCERNS IN WIRELESS SENSOR NETWORKS

Syeda Gauhar Fatimav

Professor ECE dept, Deccan College of Engineering and Technology,
Darussalam, Hyderabad, India

Syeda Kausar Fatima

Associate Professor ECE dept.,
Shadan College of Engineering and Technology, Hyderabad, India

Mohd. Mehrajuddin

Assistant Professor EIE dept., Deccan College of Engineering and Technology,
Darussalam, Hyderabad, India

Saquib Mohiuddin

Student ECE dept, Deccan College of Engineering and Technology,
Darussalam, Hyderabad, India

ABTRACT

Due to inherent limitations in wireless sensor networks, security is a crucial issue. While research in WSN security is progressing at tremendous pace, no comprehensive document lists the security issues and the threat models which pose unique threats to the wireless sensor networks. In this paper we have made an effort to document all the known security issues in wireless sensor networks and have provided the research direction towards countermeasures against the threats posed by these issues.

Keywords: wireless sensor network security, security issues in sensor networks.

1. INTRODUCTION

Sensor networks pose unique security challenges because of their inherent limitations in communication and computing. The deployment nature of sensor networks makes them more vulnerable to various attacks. Sensor networks are deployed in applications where they have physical interactions with the environment, people and other objects making them more

vulnerable to security threats. We envision that sensor networks would be deployed in mission critical applications like battlefield, security of key land marks, building and bridges, measuring traffic flow, habitat monitoring and farming. Inherent limitations of sensor networks can be categorized as node and network limitations. The privacy and security issues in sensor networks raises rich research questions. Dense deployment of sensor networks in an unattended environment makes sensor nodes vulnerable to potential attacks. Attackers can capture the sensor nodes and compromise the network to accept malicious nodes as legitimate nodes. Once within the network, attackers can rage variety of attacks. We expect Moore's law to be applied to drive down the cost of sensor nodes instead of improving its resources and performance.

Hardware and software improvements will address these issues at some extent but complete secure sensor networks require deployment of countermeasures such as secure key management, secure routing and light weight encryption techniques. This paper provides an overview of security issues known so far in wireless sensor networks.

2. LIMITATIONS IN SENSOR NETWORKS

The following section list the inherent limitations in sensor networks which make the design of security procedures more complicated.

2.1. Node limitations

A typical sensor node processor is of 4-8 MHz, having 4KB of RAM, 128KB flash and ideally 916 MHz of radio frequency. Heterogeneous nature of sensor nodes is an additional limitation which prevents one security solution. Due to the deployment nature, sensor nodes would be deployed in environments where they would be highly prone to physical vandalism.

2.2. Network limitations

Beside node limitations, sensor networks bring all the limitations of a mobile ad hoc network where they lack physical infrastructure, and they rely on insecure wireless media.

2.3. Physical limitations

Sensor networks deployment nature in public and hostile environments in many applications makes them highly vulnerable to capture and vandalism. Physically security of sensor nodes with tamper proof material increases the node cost.

3. CHARACTERISTICS OF SENSOR NETWORKS

Sensor networks are emerging technologies currently being deployed in seismic monitoring, wild life studies, manufacturing and performance monitoring. These sensor nodes are densely deployed in a predetermined geographical area to self-organize into ad-hoc wireless networks to gather and aggregate data [13]. A typical sensor network contains large number of densely deployed, tiny, low cost nodes that use wireless peer-to-peer network. They use multi-hop and cluster-based routing algorithms based on dynamic network and resources algorithms based on dynamic network and discovery protocol. [14]. For the purpose of this research we assume usage of Berkeley's Mica2Dot sensor node [16] which is limited in terms of computations and communication resources.

The ad hoc nature of sensor networks poses unique challenges with their security and reliability. Resource constrained sensor nodes in terms of limited memory; low power, limited processing abilities, and low coverage are vulnerable to intrusion, interception, modification and fabrication. Because of these unique challenges traditional security techniques are not enough to meet the security goals of confidentiality, integrity, reliability and availability. Unlike traditional networks, sensor nodes are deployed physically in open areas where there is added

risk of intervention with people and environment [15]. Therefore, new security measures are needed to address these unique sensor networks security challenges.

4. SECURITY IN SENSOR NETWORKS

Security goals in sensor networks depend on the need to know what we are going to protect. We determine four security goals in sensor networks which are Confidentiality, Integrity, Authentication and Availability (CIAA).

Confidentiality is the ability to conceal message from a passive attacker, where the message communicated on sensor networks remain confidential.

Integrity refers to the ability to confirm the message has not been tampered, altered or changed while it was on the network.

Authentication Need to know if the messages are from the node it claims to be from, determining the reliability of message's origin.

Availability is to determine if a node has the ability to use the resources and the network is available for the messages to move on.

4.1. Security classes

Pfleeger [2] has identified four classes of security in computing systems. We integrate these four threat classes in sensor networks. In computing systems the major assets are hardware, software, and data. While in sensor networks, our goal is to protect, the network itself, the nodes and communication among the sensor nodes. The four classes of threats which exploit the vulnerability of our security goals are illustrated below in Figure 1:
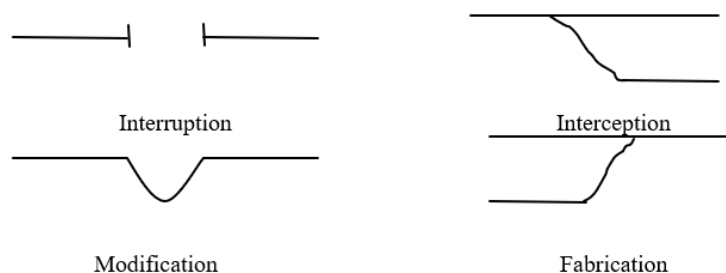

Figure 1 Pfleeger's four classes of Systems security threats

In an *interruption*, a communication link in sensor networks becomes lost or unavailable. Examples of this sort of threats are node capture, message corruption, addition of malicious code etc.

An *interception* means sensor network has been compromised by an adversary where the attacker gains unauthorised access to sensor node or data in it. Example of this type of attacks is node capture attacks.

Modification means unauthorised party not only accesses the data but tampers with it, for example modifying the data packets being transmitted causing a denial of service attack such as flooding the network with bogus data.

In *fabrication*, an adversary injects false data and compromises the trustworthiness of information.

4.2. Attacks on sensor networks

Having built a foundation of security threats in computing, next section lists the possible security attacks in sensor networks identified by [3].

4.2.1. Passive Information Gathering

An adversary with powerful resources collecting information from sensor networks if information is not encrypted.

4.2.2. Node subversion

Capture of a node may reveal its information including disclosure of cryptographic keys hence compromising the whole sensor network.

4.2.3. False Node

Addition of a malicious node by an adversary to inject the malicious data, false node would be computationally robust to lure other nodes to send data to it.

4.2.4. Node Malfunction

A malfunctioning node will generate inaccurate data which would jeopardize the integrity of sensor network especially when that node is data aggregating node for example, a cluster leader.

4.2.5. Node Outage

What happens when a cluster leader stop functioning? Sensor network protocols should be robust enough to mitigate the effects of node outages by providing alternate route.

4.2.6. Message Corruption

When contents of a message are modified by an attacker it compromises the message integrity.

4.2.7. Traffic Analysis

Even the message transfer is encrypted in sensor networks, it still leaves the high probability of analysis of communication patterns and sensor activities revealing enough information to enable adversary to cause more malicious harm to sensor networks.

4.2.8. More attacks

Chris Karlof et al [4] have presented much detailed attacks in sensor networks which are described in the following section. Table 1 below lists these attacks.

Table 1 Attacks in Wireless Sensor Networks

Spoofed, altered, or replayed routing information	Create routing loop, attract or repel network traffic, extend or shorten source routes, generate false error messages etc
Selective forwarding	Either in-path or beneath path by deliberate jamming, allows to control which information is forwarded. A malicious node act like a black hole and refuses to forward every packet it receives.
Sinkhole attacks	Attracting traffic to a specific node, e.g. to prepare selective forwarding
Sybil attacks	A single node presents multiple identities, allows to reduce the effectiveness of fault tolerant schemes such as distributed storage and multipath etc.
Wormhole attacks	Tunnelling of messages over alternative low-latency links to confuse the routing protocol, creating sinkholes etc.
Hello floods	An attacker sends or replays a routing protocols hello packets with more energy

4.2.9. Routing loops

In sensor networks routing loops attacks target the information exchanged between nodes. False error messages are generated when an attacker alters and replays the routing information. Routing loops attract or repel the network traffic and increases node to node latency.

4.2.10. Selective forwarding

Selective forwarding is a way to influence the network traffic by believing that all the participating nodes in network are reliable to forward the message.   In selective forwarding attack malicious nodes simply drop certain messages instead of forwarding every message. Once a malicious node cherry picks on the messages, it reduces the latency and deceives the neighboring nodes that they are on a shorter route.   Effectiveness of this attack depends on two factors. First the location of the malicious node, the closer it is to the base station the more traffic it will attract. Second is the percentage of messages it drops. When selective forwarder drops more messages and forwards less, it retains its energy level thus remaining powerful to trick the neighboring nodes.

4.2.11. 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.

4.2.12. Sybil attacks

A type of attacks where a node creates multiple illegitimate identities in sensor networks either by fabricating or stealing the identities of legitimate nodes. Sybil attacks can be used against routing algorithms and topology maintenance; it reduces the effectiveness of fault tolerant schemes such as distributed storage and dispersity. Another malicious factor is geographic routing where a Sybil node can appear at more than one place simultaneously.

4.2.13. Wormholes

In wormhole attacks an adversary positioned closer to the base station can completely disrupt the traffic by tunneling messages over a low latency link. Here an adversary convinces the nodes which are multi hop away that they are closer to the base station. This creates a sinkhole because adversary on the other side of the sinkhole provides a better route to the base station.

4.2.14. Hello flood attacks

Broadcasting a message with stronger transmission power and pretending that the HELLO message is coming from the base station. Message receiving nodes assume that the HELLO message sending node is the closest one and they try to send all their messages through this node. In this type of attacks all nodes will be responding to HELLO floods and wasting the energies. The real base station will also be broadcasting the similar messages but will have only few nodes responding to it.

4.2.15. DoS attacks

Denial of service attacks occur at physical level causing radio jamming, interfering with the network protocol, battery exhaustion etc.

4.3. Layering based security approach 1) Application layer

Data is collected and managed at application layer therefore it is important to ensure the reliability of data. Wagner [6] has presented a resilient aggregation scheme which is applicable to a cluster based network where a cluster leader acts as an aggregator in sensor networks. However this technique is applicable if the aggregating node is in the range with all the source nodes and there is no intervening aggregator between the aggregator and source nodes. In hierarchical clustering approach, communication channel between the aggregator and base station has potentially limited bandwidth because the cluster leader as an aggregator itself is a sensor node [5, 6]. To prove the validity of the aggregation, cluster leaders use the cryptographic techniques to ensure the data reliability.

4.3.1. Network Layer

Network layer is responsible for routing of messages from node to node, node to cluster leader, cluster leaders to cluster leaders, cluster leaders to the base station and vice versa.

Routing protocols in sensor networks are of two types (1) ID-based protocols, in which packets are routed to the destination based on the IDs specified in the packets, and (2) data centric protocols [7] in which packets contain attributes that specify the type of data being provided. Law and Havinga [5] have described Karlof and Wagner's [4] routing attacks in sensor networks as below:
- Packets are dropped completely, or selectively.
- The network is flooded with global broadcasts.
- Some sensor nodes in the network are misguided into believing that nodes are either multiple hops away or that do not exist at all in the neighbours.
- A significant proportion of the traffic is tunnelled from one place in the network to another distant place of the network depriving other parts of the network that under normal circumstances would have received the traffic themselves.
- Sometimes traffic is lured to a particular node or a small group of nodes, depriving other parts of the network that normally would have received the traffic themselves.
- Security of routing protocols depends on the location of nodes and the encryption techniques.

4.3.2. Data Link layer

Data link layer does the error detection and correction, and encoding of data. Link layer is vulnerable to jamming and DoS attacks. TinySec [9] has introduced link layer encryption which depends on a key management scheme. However, an attacker having better energy efficiency can still rage an attack. Protocols like LMAC [8] have better antijamming properties which are viable countermeasure at this layer.

4.3.3. Physical Layer

The physical layer emphasizes on the transmission media between sending and receiving nodes, the data rate, signal strength, frequency types are also addressed in this layer. Ideally FHSS frequency hopping spread spectrum is used in sensor networks.

Table II below summarizes the attacks and countermeasures in a layering model in sensor networks.

Table 2 Layering Approach In Sensor Network Attacks And Countermeasures

	Attack types	Countermeasures
Application Layer	Subversion and Malicious Nodes	Malicious Node Detection and Isolation
Network Layer	Wormholes, Sinkholes, Sybil, Routing loops	Key Management, Secure Routing
Data Link Layer	Link layer Jamming	Link layer encryption
Physical Layer	DoS and Node capture attcks	Adaptive antennas, Spread Spectrum

5. CONCLUSION

Wireless Sensor networks have become promising future to many applications. In the absence of adequate security, deployment of sensor networks is vulnerable to variety of attacks. Sensor node's limitations and nature of wireless communication poses unique security challenges. Current research in sensor network security is mostly built on a trusted environment [12]; however there are several research challenges remain unanswered before we can trust on sensor networks. In this paper we have discussed threat models and unique security issues faced by wireless sensor networks. On the basis of our observation we motivate the need of a security framework to provide countermeasures against attacks in wireless sensor networks.

REFERENCES

[1]   L. Eschenauer and V. Gligor, A key-management scheme for distributed sensor networks, *Proceedings of the 9th ACM conference on Computer and Communication Security 2002*, Washington DC, USA

[2]   C.P. Fleeger, Security in computing, 3rd edition, *Prentice-Hall Inc*. NJ. 2003

[3]   J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, Security for sensor networks, 2002 CADIP *Research Symposium.*

[4]   C. Karlof and D. Wagner, Secure routing in wireless sensor networks: Attacks and Countermeasures, *Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, Vol. 1, No. 2-3, pp. 293-315, 2003.

[5]   Y.W. Law and P. J.M Havinga, How to secure sensor network, *Proceeding of the 2005 International Conference on Sensor Networks and Information Processing*, 5-8 Dec. 2005 pp. 89-95

[6]   D. Wagner, Resilient aggregation in sensor networks, *In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*. ACM Press, 2004, pp. 78-87.

[7]   D. Ganesan, A. Cerpa, Y. Yu, and D. Estrin, Networking issues in wireless sensor networks, *Journal of Parallel and Distributed Computing (JPDC), Special issue on Frontiers in Distributed Sensor Networks*. Vol. 64, 2004.

[8]   L.V. Hoesel and P. Havinga, A Lightweight Medium Access Protocol (LMAC) for wireless sensor networks: reducing preamble transmissions and transceiver state switches, *in the proceedings of INSS*, June 2004.

[9]   C. karlof, N. Shastry and D. Wagner, TinySec: A link layer security architecture for wireless sensor networks, *SenSys'04*, November 3-5 2004, Baltimore, Maryland, USA

[10]   H. Chan, A. Perrig, Security and privacy in sensor networks, *IEEE Journal of Computing*, Vol. 36, Issue 10, Oct. 2003, pp. 103-105

[11]   F. Stajano, Security for Ubiquitous Computing, *John Wiley and Sons*, NY 2002, ISBN:0-470-84493-0

[12]   E. Shi, and A. Perrig, Designing secure sensor networks, *Journal of IEEE Wireless Communications*, Vol. 11, Issue 6, Dec. 2004 pp 38-43.

[13]   N. Hu, Randy R. K. Smith and P. G. Bradford, Security for Fixed Sensor Networks, *Proceedings of the 42nd annual Southeast regional conference, ACM Press*, 2004, NY, USA

[14]   R. Anderson, H. Chan, and A. Perrig, Key infection: smart trust for smart dust, *12th IEEE International Conference on Network Protocols*. Oct 5-8 2004, Berlin, Germany

[15]   A. Perrig, J Stankovic, D. Wagner, Security in wireless sensor network, *Communication of the ACM*, Vol.47, No. 6, 2004

[16]   Wireless   sensor   networks: getting started guide, *Crossbow Technology, Inc, San Jose, CA*, Aug'04.   http://www.xbow.com/Support/Support_pdf_files/Gettin g_Started_Guide_7430-0022-05_B.pdf [Viewed online 10 June 2006]

[17]   Deepak. S. Sakkari and Dr. T. G. Basavaraju, Optimized Coverage and Connectivity for Randomly Deployed Wireless Sensor Network for Lifetime Conservatory, International Journal of Computer Engineering and Technology (IJCET), Volume 4, Issue 6, November - December (2013), pp. 247-255

[18]   Sachin Gajjar, Mohanchur Sarkar and Kankar Dasgupta, Performance Analysis of Clustering Protocols For Wireless Sensor Networks, International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 4, Issue 6, November - December, 2013, pp. 107-116

[19]   Er. Harjot Kaur, Dr. Gaurav Tejpal and Dr. Sonal Sharma, Performance Evaluation of NSGA-III Based Energy Efficient Protocol for Wireless Sensor Networks, International Journal of Mechanical Engineering and Technology 8(9), 2017, pp. 325–336.

[20]   Basavaraj S. Mathapati, Siddarama. R. Patil and V. D. Mytri, Power Control with Energy Efficient and Reliable Routing Mac Protocol For Wireless Sensor Networks, International Journal of Computer Engineering and Technology (IJCET), Volume 3, Issue 1, January- June (2012), pp. 223-231