Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 7, July 2013, pg.422 – 426

RESEARCH ARTICLE

Overview of Security Threats in WSN

Ms. Poonam Barua[1], Mr. Sanjeev Indora[2]
[1]M. Tech (Final year), CSE Department, DCRUST Murthal (131039), India
[2]Assistant Lecturer, CSE Department, DCRUST Murthal (131039), India

[1] poonambarua6@gmail.com; [2] sanjeev.cse@dcrustm.org

Abstract— Wireless sensor network is a combination of tiny devices called as sensor nodes which have computing, sensing and processing capabilities. As WSN are deployed in hostile environment usually and can be physically accessible by an adversary; he/she can affect the confidentiality and integrity of the data as well as some other security measures. So security is a main concern in wireless sensor network especially in hostile environment. In this paper we focus on security requirements, security schemes, threats, attacks and their countermeasures that provide protection from those attacks.

Key Terms: - Wireless Sensor Network; Security Requirements; Layer-based Attacks; Countermeasures; Cryptography in WSN

I. INTRODUCTION

WSN (Wireless Sensor Network) have gained much popularity and attention over the last few years. One of the reasons for its popularity has been its usage in critical applications like military application (battlefield surveillance), habitat monitoring, weather forecasting, health monitoring etc. A WSN can be considered a special type of Ad-hoc network composed of a large no. of very small, cheap and highly constrained sensor nodes [1, 17-19]. Sensors in WSN can be used to gather and process the data from the surrounding environment (e.g. mechanical, thermal, optical, biological and chemical readings) [2]. WSN is usually designed to have sink node (base station) and many simple sensor nodes. Sensor nodes sense some data/readings and send it to sink node. Then, Sink node performs some computation on received data to infer some meaningful data [1]. Depending on the hardware, wireless sensor network can be either homogeneous (all nodes are alike) or heterogeneous (nodes with different resources exist). Also, depending on the roles performed by each node, WSNs can be classified as distributed (all nodes are alike) or hierarchical (depending on its capacity, each node perform different role) [2]. Source to sink link communication is very crucial for many critical applications like health care and military. Therefore, source to sink communication should be secure and reliable. Since, sensor nodes are usually deployed in a hostile environment and are therefore prone to various malicious attacks. This is the reason that WSN's Security has been an important issue for researchers for the last few years [1].

II. OVERVIEW OF SECURITY ISSUES

Security attack is a concern for WSN because:

- Wireless communication of the system device
- Use of resource constrained devices in the network like memory, energy, computation constraints sensor nodes.
- Physical inaccessibility to sensor devices.

So, to protect the confidential information from hackers, it is necessary to provide secure communication b/w sensor nodes and base station.

A. Security Requirements

The goal of security scheme in WSN is to protect confidential information from various attacks. Security requirement in WSN are as follows [3-5]:

- *Confidentiality:*

It means disclosure of data should be protected from unauthorized parties by the security scheme.

- *Integrity:*

It means no data modification during transmission. In term of security scheme, it means keys should be accessible to the nodes in the network only.

- *Authenticity:*

It ensures that data received is originated from correct resource.

- *Node repudiation*:

It means preventing malicious nodes to hide their activities.

- *Availability:*

It means ensuring that the service offered by whole WSN, by any part of it, or by a single sensor node must be available whenever required.

- *Scalability:*

Security technique should provide high security to smaller network and should maintain that for larger network too.

- *Flexibility:*

It means when nodes become compromised, they should be replaced.

- *Data Freshness:*

It means that old data/keys should not be used as new.

- *Survivability:*

It means ability to provide a minimum level of service in the presence of power loss, failures or attacks.

- *Robustness:*

Sensor network should be strong enough to prevent attacks.

- *Self-organization:*

Nodes should be so much flexible that they are able to self-organize and self-heal.

- *Secure localization*:

It means nodes should acquire location information securely as well as accurately.

- *Time synchronization*:

Security protocols should not be manipulated to produce incorrect data.

B. Key issues for achieving the security in WSN [6]

Following four key issues have been identified for providing security to the WSNs and they are based on the analysis on security challenges and potential attacks and are as follows:

1) Key management in WSN:

TABLE I. Any key management scheme should support at least confidentiality, authenticity and integrity. But because of various resource constraints in WSN, it is difficult to provide key management service.

2) Encryption and Decryption scheme:

TABLE II. Due to resource constrained nature of WSN, Encryption and Decryption scheme must be simple and energy efficient.

3) *Secure routing of WSN:*

TABLE III. Major two types of attack in WSN:

- *External attack*- External attacker may partition a network or put extra load on the network. E.g. - injection of erroneous routing information, replaying old information. Cryptographic technique can help in it.
- *Internal attack*- Any compromised node may do internal attack. It is difficult to put defense against these attacks.

4) *Prevention of Denial-of-Service (DOS)*: DOS attack diminishes a net work's capacity to perform its expected function.

III. LAYER-BASED ATTACKS [4,7]

A. Physical layer:

Communication media is wireless (open), so high security risk is there. Some of those security threats are:

JAMMING: It is a popular Denial of service (DOS) attack on physical layer of network. In jamming, adversaries interferes with the communication frequencies (radio frequencies) being used by the nodes of the network. In jamming, an attacker can simultaneously transmit over the WSN refusing the underlying MAC

protocol. Jamming can affect the whole n/w if single frequency is used throughout the n/w and also it can cause excessive energy consumption at any node if impertinent packets are injected. By getting those packets receiver's nodes will as well consume energy [4, 8].

Xu, Trappe, Zhang and wood in 2005 proposed [4, 9] four different Type of jamming attacks which may be used by an adversary to stop the operation of a WSN.

TAMPERING: It is another physical layer attack. In this type of attack, an adversary may compromise some of the legitimate sensor nodes in the network and using these nodes, he/she may carry out lots of misleading activities in the network.

SYBIL ATTACK: An adversary node assumes identity of multiple nodes. This may causes ineffectiveness in WSN. Sybil attacks the network with:

- Fault tolerance
- Geographic routing protocol

In table 1, describes various physical layer attacks and their countermeasures in WSN [4, 10].

TABLE I. Physical Layer Threat and Countermeasures

Threats	**countermeasure of threats**
Jamming	Prioritize messages, Jamming the Spread-spectrum, lower the duty cycle, mode change, channel hoping and blacklisting.
Tampering	Tamper-proofing, hiding, protection.
Sybil attack	Physical protection of devices
Interference	Channel hoping and blacklisting

B. Data link layer:

Attacks can also be made on data link layer. Various data link layer threats are as follows [6]:

COLLISION: In this type of DOS attack, an adversary may induce small change in data portion of the packet and which may lead to error in checksum calculation and may cause retransmission of data packets.

EXHAUSTION: In this type of attack, an adversary may continuously disturb the communication between two nodes and causes the sensor node to retransmit continuously. This may lead to quick energy decay.

TRAFFIC ANALYSIS: Communication pattern of a sensor network can be analyzed by an adversary to cause harm to the network.

SYBIL ATTACK: This type of attack is very much effective in link layer. Different variation of Sybil attacks are:

- Data aggregation- A single malicious node may act as different Sybil nodes and these may give many negative reinforcements to make the aggregate message a false one.
- Voting: An attacker may be able to determine the outcome of any voting depending on the no. of identities the attacker owns.

SPOOFING: After overhearing the packets, an adversary can spoof link layer acknowledgements.

TABLE II. Link layer threats and countermeasure

Threats	**Countermeasures**
Collision	Error correcting code, CRC and time diversity
Exhaustion	Rate limitation and protection of network ID
Spoofing	Using different path for re-sending the messages.
Sybil attack	Changing the keys regularly
Traffic analysis	Regularly monitoring WSN network by sending dummy packets in quite hours.
Eavesdropping	Keys protects from eavesdropper

C. Network layer:

Major security goal of network layers are [6]:

- Every intended receiver node should receive all messages intended to it and also should verify the ID of source node and integrity of message.
- Routing protocol should be responsible for preventing eavesdropping.

WSN network layer are vulnerable to various attacks. Broadly, they are categorized in two types [4]-

- *Passive attack*- An adversary can only discover information without modifying them. It is difficult to detect these attacks.
- *Active attack*- An adversary can modify/falsify the information and thus interfere in functioning of the network. An attacker can modify both routing as well as data packets causing false routing table at

source and imperfect communication. E.g. – Wormhole attack [11], Black hole attacks [12], Byzantine attacks [13], DDOS attacks [14], Routing attacks [15, 20].

Encryption scheme and hash functions can be used to provide authenticity and integrity of data. Table 3 describes various network layer threats and countermeasures [10].

TABLE III. Network layer threats and countermeasures

Threats	Countermeasures
Eavesdropping	Session keys protects from eavesdropper
Sybil	Changing of keys and resetting of devices
Selective forwarding	Regular monitoring of network using source routing
Traffic analysis	Regularly monitoring WSN network by sending dummy packets in quite hours.
DOS	Physical protection of network and protection of n/w specific data-link n/w ID.
Wormhole attack	Controlling and verifying hop count. This will limit the self-organizing nature of an ad-hoc network. Use protocol that is not based on hop count. Regular monitoring of network using source routing.

D. Transport layer:

Threats present on transport layers are [6]:

FLOODING ATTACK: e.g. – TCP SYN flood attack. In this, an adversary continuously sends the connection requests and floods the network link at targeted node.

DE SYNCHRONIZATION: A pair of nodes can be made to stick in synchronization recovery protocol by maintaining proper timing and disrupting some of the packets transmitting in b/w the nodes.

Table 4 describes various transport layer threats and countermeasures.

TABLE IV. Transport layer Threats and Countermeasures

Threats	Countermeasures
Flooding attack	Client puzzles
De synchronization	Authentication

IV. CRYPTOGRAPHY IN WSN

WSN are used in many critical applications like military, habitat monitoring etc. Minimum level of security like integrity and authentication is required for certain applications, due to their sensitive nature of data. This type of security can be provided by using any cryptography scheme in WSN. Cryptography aims at making data not understandable to any unauthorized party which has the goal of data interpretation. But, it is difficult to choose the appropriate scheme because of resource/computation constrained nature of WSN. PKC (Public key cryptography) is not suitable for WSN because of its resource demanding nature [1, 16]. SKC (symmetric key cryptography) is more efficient and suitable for WSN. But, it has the inherent problem of sharing the secret keys and also, the hostile nature of WSN makes it vulnerable to various attacks [1, 16].

In order to encrypt or decrypt data, first of all keys should be distributed among nodes. This is the goal of key management system. It is also responsible for revoking and refreshing keys in order to gain better security. For any key establishment technique to be efficient, it should support several requirements like in-network processing and facilitating self-organization of data. However, Key establishment technique should minimally support authenticity, confidentiality, integrity, flexibility and scalability [3].

V. CONCLUSION

Providing security in a wireless sensor network is a challenging task. In this paper, we have discussed various security threats present at different layer of WSN protocol stack. Possible solution against each threat is also outlined. Detection and countermeasures of some threats in WSN is not at all easy. Key distribution among sensor nodes is also a challenging task. In present time, most of the security schemes are based on specific network models and complete security model for all layers is not at all present although, in future, the security scheme might become well established for individual layer.

REFERENCES

[1] Ali Tufail, Ki-Hyung Kim, "A Backbone Assisted Hybrid Key Management Scheme for WSN", IEEE 978-0-9564263-8/3 (2011).

[2] Marcos A. Simplício Jr., Cintia B. Margi, Paulo S.L.M. Barreto, Tereza C.M.B. Carvalho, " A survey on key management mechanisms for distributed wireless sensor networks", Computer Networks 54 2591–

2612 (2010).
[3] Yang Xiao, Venkata Krishna Rayi , Bo Sun , Xiaojiang Du , Fei Hu ,Michael Galloway, "A survey of key management schemes in wireless sensor networks", Computer Communications 30 (2007) 2314–2341.
[4] Hero Modares, Rosli Salleh, Amirhossein Moravejosharieh, "Overview of Security Issues in Wireless Sensor Networks" ,2011 Third International Conference on Computational Intelligence, Modelling & Simulation.
[5] JOHNSON C. LEE AND VICTOR C. M. LEUNG, UNIVERSITY OF BRITISH COLUMBIA KIRK H. WONG, JIANNONG CAO, AND HENRY C. B. CHAN, "KEY MANAGEMENT ISSUES IN WIRELESS SENSOR NETWORKS: CURRENT PROPOSALS AND FUTURE DEVELOPMENTS ", IEEE wireless communications (2007).
[6] Hiren Kumar, Avijit Kar, Deva Sarma, " Security Threats in Wireless Sensor Networks", IEEE 1-4244-01 74-7 (2006).
[7] Syed Muhammad Khaliq-ur-Rahman Raazi, Zeeshan Pervez and Sungyoung Lee, "Key Management Schemes of Wireless Sensor Networks: A Survey".
[8] H.-J. Kim, et al., "A method to support multiple interfaces mobile nodes in PMIPv6 Domain," Presented at the proceedings of 2nd International Conference on Interaction Sciences, (Seoul) Korea (2009).
[9] W. Xu, et al., "The feasibility of launching and detecting jamming attacks in wireless networks", pp. 46-57 (2005).
[10] H. K. Kalita and A. Kar, "Wireless sensor network security analysis", (IJNGN), vol. 1, pp. 1–10 (2009).
[11] Y. C. Hu, et al., "Packet leashes: a defense against wormhole attacks in wireless networks", pp. 1976-1986 vol. 3 (2003).
[12] H. Deng, et al., "Routing security in wireless ad hoc networks", Communications Magazine, vol. 40, pp. 70-75 (2002).
[13] B. Awerbuch, et al., "An on-demand secure routing protocol resilient to byzantine failures", pp. 21-30 (2002).
[14] W. Enck, et al., "Exploiting open functionality in SMS-capable cellular networks", pp. 393-404 (2005).
[15] Y. C. Hu, et al., "Rushing attacks and defense in wireless ad hoc network routing protocols", pp. 30-40 (2003).
[16] Huan-Chung Lin and Yuh-Min Tseng, "A Scalable ID-Based Pair wise Key Establishment Protocol for Wireless Sensor Networks" , Journal of Computers (2008).
[17] J. Elson, K. Römer, Wireless sensor networks: a new regime for time synchronization, SIGCOMM Computers and Communication Reviews 33 (1) (2003) 149–154.
[18] P. Santi, Topology control in wireless ad hoc and sensor networks, ACM Computers and Survey 37 (2) (2005) 164–194.
[19] J. Yick, D. Ghosal , B. Mukherjee, "Wireless sensor network survey", computer networks 52 (12) 2292–2330 (2008).
[20] Y. C. Hu, et al., "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks", ad hoc networks, vol. 1,pp. 175-192 (2003).

