

WIRELESS SENSOR NETWORK LAYER BASED SECURITY ANALYSIS: ATTACKS AND THEIR ANTIDOTES

Naveen Kumar Gupta
M.Tech (DWCE), Suresh Gyan Vihar University Jaipur
nvngpt888@gmail.com

Abstract - At the present time, wireless sensor network (WSN) is the most developing technology in the field of electronics and communication. Wireless sensor network (WSN) consists of a large number of tiny sensor, which sense the data from physical world, do calculation and communicate with other sensors. WSN was originally motivated by military and homeland security applications such as battlefield surveillance. Now WSNs are also widely used in civilian application areas, including industrial sensing, environment and habitat monitoring, health-care applications, home automation, and traffic control. WSNs affected from several compulsions, including low data processing, poor memory, bounded energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. These compulsions make security in WSNs a challenge. In this article, we outline security demand, attacks and disputes in WSNs. We identify the security risk; analyze protection technique for wireless sensor networks. Here we also deliberate the complete view of layer based security issues and their countermeasure in WSNs.

Keywords: Security, WSNs, Challenge, Threats, Attack.

I. INTRODUCTION

Wireless sensor networks are combination of small sensors and some computing element. WSNs security is quite different from traditional network security technique, because of two major compulsions; lack of data storage and limited power. WSNs also suffer from physical attacks like node capture and tampering. The unreliable communication channel and unattended operation makes the security defenses even harder. For a complete secure network, we must provide the security at every node. WSNs must support all security objectives such as availability, authenticity, access control integrity and confidentiality.

First of all we discuss about the architecture of WSN and component of sensor node to understand why security is necessary for WSN.

II. WSN ARCHITECTURE

a) Network Manager: Main task of network manager is to build up the network, manage communication, control routing chart, check and report network strength. In short we say that it configure the super frame.

b) Internet: Internet is basically the unreliable communication channel. It enables the communication between network manager and gateway. In this communication channel, a great possibility of attacks, so we need a security manager which provides the security.

c) Security Manager: It is responsible for the making, storage and managing the keys.

d) Gateway: It makes connection between Host application and sensor nodes.

e) Sensor Nodes: Sensor nodes are mounted in the route and must be able of routing packets on behalf of other devices. Mostly they describe and direct the

process or process devices. A router is a special type of field device that used for transfer the packet from one node to another.

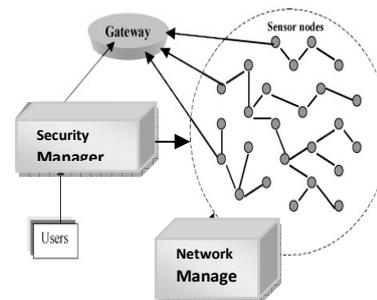


Figure 1. WSN ARCHITECTURE

III. ARCHITECTURE OF SENSOR NODE

A Wireless Sensor Network consists of large number of sensors nodes. In a sensor field these sensor nodes are often closely deployed and have the ability to collect data and route data back to a base station. There are basically four parts of a sensor node:-

- Sensing Unit,
- Computing unit,
- Communication Unit and
- Power Unit

a) Sensing Unit:

Sensing unit further divided into two subunits: sensor and analog to digital converters (ADC). Sensors sense the data from physical environment, do calculation and produce an analog signal. The ADC converts these analog signals into digital signals based on the observed phenomenon.

b) Computing unit:

A computing unit generally consist a processor, a limited memory and some protocols. The sensor node collaborated with the other nodes, which is managed by processor unit. Like traditional wired network system the processors of WSNs are not powerful, so we cannot used a complex algorithm. Memory unit includes RAM and Flash memory, these are not sufficient to execute a complex algorithm. RAM is responsible for storing sensor data, intermediate computation and application program, while Flash memory is responsible for storing downloaded application code.

c) Communication unit:

A transceiver antenna is used for communication between node and network. Communication range of sensor nodes is

limited. The strength of transmitted depends on weather conditions and environment.

d) Power unit:

Power unit is the most important part of sensor node; it may be a battery or a solar panel.

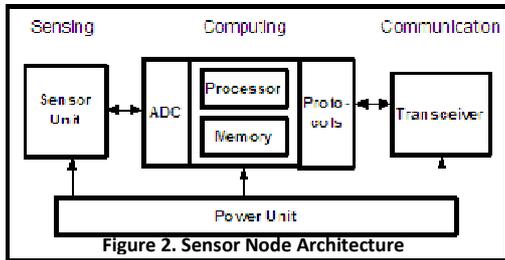


Figure 2. Sensor Node Architecture

IV. SECURITY REQUIREMENT

The attackers organized the fake sensor nodes with same configuration and hardware for a mutual attack on the network channel. Then the attackers physically capture or reprogrammed the actual node using the phony sensor nodes. The genuine nodes have not a robust security, so the attackers easily replace the phony nodes and access all data, code and keys. A robust security is the solution to protect the original nodes.

To protect the information and resources from attacks and misbehavior some security services are required for WSNs. WSNs must support all security objectives such as availability, authenticity, integrity and confidentiality.

a) Availability:

The entire yearned sensor network services are available during communication.

b) Authentication

It makes sure that only correct resource originated the data. It is also responsible for a genuine communication between two nodes, i.e., a fake node cannot cover-up as a trusted node.

c) Integrity:

It makes sure that a message sent from one sensor node to another is not modified by fake intermediate nodes.

d) Confidentiality:

It makes sure that only desired receiver understood the received message.

e) Robustness:

To prevent attacks, Sensor network should be strong enough.

V. ANALYSIS OF LAYER-BASED ATTACKS

PHYSICAL LAYER SECURITY ISSUES

- a) Sybil Attack
- b) Interference
- c) Jamming
- d) Tampering

a) Sybil Attack:

In the Sybil attack, one adversary sensor nodes assumes multiple identities to all other sensor nodes in the WSN. This reduces the effectiveness of WSN. We must protect the physical devices to prevent

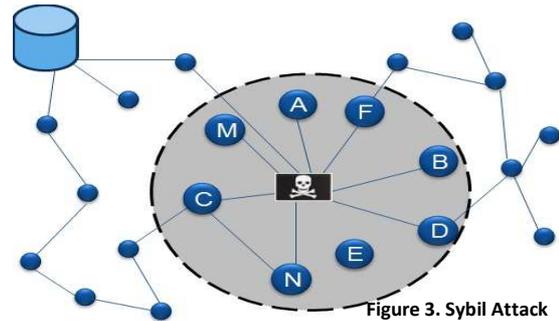


Figure 3. Sybil Attack from

Sybil attack. Sybil attack affected the following protocols and algorithms:

- Network topology maintenance
- Fault-tolerant
- Distributed storage
- Geographic routing protocol

b) Interference:

In this attack an adversary sensor node only require to produce a collision/interference in the transmission. To remove this issue blacklisting and channel hopping are used.

c) Jamming:

In this attack adversary nodes disrupt the communication frequencies of required sensor network. Thus the communication channel is Jammed. It is also known as denial of service attack. If only one frequency is used throughout the network then jamming can affect the whole sensor network. Due to this, Energy consumption is increased at nodes. To handle these Issues symmetric key algorithms are used. Antidote of jamming is lower the duty cycle, prioritize messages, Jamming the Spread-spectrum, mode change, channel hopping and blacklisting.

d) Tampering:

In this attack, Attacker can take out sensitive information like message or cryptographic key. The sensors nodes are also tempered or swap to create a fake node which the attacker operates. To remove this issue Tamper-proofing, hiding and protection are required.

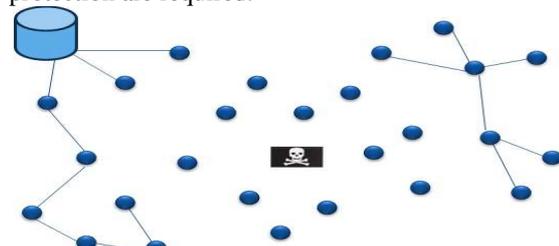


Figure 4. Jamming Attack

DATA LINK LAYER SECURITY ISSUES

- a) Collision
- b) Exhaustion
- c) Spoofing
- d) Sybil attack
- e) traffic Analysis

a) Collision:

It is a Denial of Services (DOS) attack, attacker induces minute change in data packet will result in checksum mismatch. This may cause retransmission of data packets. Then the packets will be rejected as invalid. To avoid

collision, error correcting code, CRC and time diversity techniques are used.

b) Exhaustion:

The communication between two nodes is continuously disturbed using repeated collision by an attacker. Due to Exhaustion the nodes are continuously retransmit the data that's why energy quickly decrease. To avoid Exhaustion, we must protect the network ID and limited the data rate.

c) Spoofing:

In the sensor network, the attacker may spoof, alter, or rerun routing algorithm so as to interrupt the network traffic. An attacker is able to spoof link layer acknowledgements, after overhearing the packets. This issue can be resolve by using different path for re-sending the messages.

d) Sybil Attack:

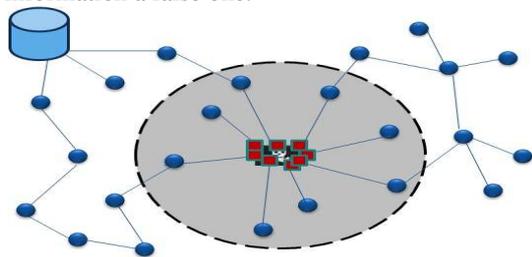
In link layer, Sybil attack is greatly effective. To block the Sybil attack at link layer we have to change the security keys regularly. This is a popular attack of DOS. There are two types of Sybil attacks in the link layer:

A. Voting:

An adversary may be able to find out the outcomes of any voting depending on the number of identities of the adversary owns.

B. Data Aggregation:

A spiteful node may act as dissimilar Sybil nodes and these may give much harmful reinforcement to make the collective information a false one.



e) Traffic Analysis: Figure 5. Collision Attack

An attacker analyzed the communication channel of sensor network to damage to the sensor network.

NETWORK AND ROUTING LAYER SECURITY ISSUES

Security requirement of network layer:

- Each receiver Node receives all intended message then verify the ID of source node and integrity of message.
- For preventing eavesdropping, routing protocol should be responsible.
- Networks are generally data – centric.

Attacks in network and routing layer:

- a) Wormhole
- b) Sybil
- c) Sinkhole
- d) Selective forwarding
- e) Hello Flood Attack
- f) Acknowledge spoofing

a) Wormhole:

An attacker can received channel messages in a particular area of the network above a low delay link and repeat them in another branch of the network. This is done by the coordination of two opponent node. Wormhole attacks usually occupy two isolated nodes that are colluded to underrate the space between them and send packets through a peripheral communication channel that is only presented to the opponent. To prevent this attack we must be use protocol i.e. not based on hop count. We also control and verify hop count, packet bridles by using geographic and sequential information.

b) Sybil Attack:

In the Sybil attack, one adversary sensor nodes assumes multiple identities to all other sensor nodes in the WSN. This reduces the effectiveness of WSN. A fake node appears at several places at same time. Sybil attacks are prevented by changing the security keys and resetting the network devices.

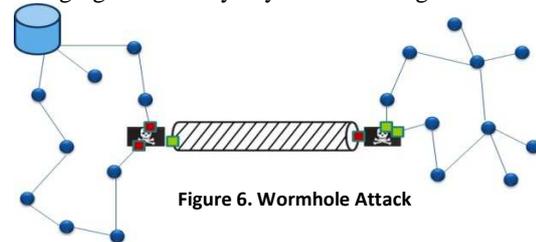


Figure 6. Wormhole Attack

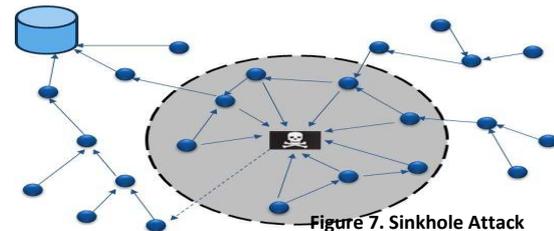


Figure 7. Sinkhole Attack

c) Sinkhole:

Here an attacker makes a compromised node stare more attractive to adjacent nodes by unfaithful routing information. A malevolent sensor node works as a blackhole to attract the entire traffic network. That's why Sinkhole attack is also called Black hole attack.

d) Selective Forwarding:

In the multihop networks all nodes exactly forward received data, but the attacker developed a malevolent sensor nodes which selectively forward only certain data and drop others data. There are two methods to protection from Selective Forwarding:

- Using several paths to send data and
- Detect the malevolent sensor node then disastrous.

e) Hello Flood:

Several routing protocols in WSN require nodes to transmit HELLO packet to broadcast themselves to their neighbors. The sensor node which accepts such a message may suppose that it is inside a radio range of the sender. On the other hand in some cases this hypothesis may be phony; sometimes a laptop-class-attacker spreading routing or other message with sufficient broadcast power could encourage all other node in the network that the attacker is its neighbor. To prevent the Hello flood attack, Authentication and verification of bidirectional link are required.

f) Acknowledge Spoofing:

Sometimes acknowledge are required in routing algorithm used by sensor network. An adversary node can spoof the Acknowledgments of overheard packets intended for adjacent nodes in order to supply fake message to those adjacent nodes.

TRANSPORT LAYER SECURITY ISSUES

Transport layer manages the end-to-end connection. There are two attacks in transport layer:

- a) Flooding
- b) De synchronization

a) Flooding:

An adversary continuously makes new connection requests and floods the network link at objective node. To overcome this problem we use a client puzzles

b) De Synchronization:

A few nodes can be completed to attach in harmonization recovery protocol by maintaining the appropriate timing and disorderly some of the packets transmitting in the nodes. The countermeasure of this attack is Authentication.

VI. PROPOSED CONCEPT OF ANTIDOTES IN WSNs

We assigned a node ID to each node in WSNs and the range of node ID is [1, n]. Suppose an attacker placed a phony node with same range node ID in the sensor network for an attack over the routing protocol. Now we perform a repeated node ID hopping within the given range and produce a new set of Node ID. So that routing contradiction of the phony node become quite complex.

This concept is very simple but much proficient countermeasure to Denial of service (DOS) and network incursion. In this solution no need of routing table.

VII. Conclusion

In this article we have discussed about architecture of WSNs and sensor node, security attacks and their countermeasure. Security attacks are still a big challenge. Asymmetric Key cryptography has ability to solve many security issues, but in WSN the sensor node has small memory and power that's why asymmetric key not used. The Sinkhole and Wormholes creates a lot of challenge to protect the routing protocol proposal. The detection and solution of these attacks are not easy. At present day projected defense proposals are based on particular network models. Since there is a lack of pooled stab to get an ordinary model to guaranteed security for every layer, after this the security performance become well-set up for each particular layer in future, combining all the mechanisms jointly for building them work in cooperation with each other will acquire a hard research challenge.

VIII. REFERENCES

- [1] C hris Karlof and David Wagner. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols. 2003.
- [2] Wood, A. D., & Stankovic, J. A. (2002). Denial of service in sensor networks. *IEEE Computer*, 35(10), 54-62.
- [3] Du, W., Deng, J., Han, Y.S., & Varshney, P. K. (2003). *A pairwise key pre-distribution scheme for wireless sensor networks*. In Jajodia (pp. 42-51).
- [4] J. Kulik, W. R. Heinzelman, and H. Balakrishnan Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks. *Wireless Networks*, vol. 8, no. 2-3, pp. 169-185, 2002.
- [5] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, System Architecture Directions for Networked Sensors, ASPLOS, November 2000.
- [6] Culler, D. E and Hong, W., "Wireless Sensor Networks", *Communication of the ACM*, Vol. 47, No. 6, June 2004, pp. 30-33.
- [7] A.D. Wood and J.A. Stankovic, (2002) "Denial of Service in Sensor Networks," *Computer*, vol. 35, no. 10, 2002, pp. 54- 62.
- [8] Dr. Moh. Osama K., (2007),Hello flood counter measure for wireless sensor network, *International Journal of Computer Science and Security*, volume (2) issue (3)
- [9] J. Yick, D. Ghosal , B. Mukherjee, "Wireless sensor network survey", *computer networks* 52 (12) 2292-2330 (2008).
- [10] Luis E. Palafox, J. Antonio Garcia-Macias,(2008) *Security in Wireless Sensor Networks*, IGI Global, Chapter 34.
- [11] Chowdhury M, Kader M F, Asaduzzaman. Security Issues in Wireless Sensor Networks: A Survey. *International Journal of Future Generation Communication and Netwrking*, ISSN: 2233-7857 IJFGCN , Vol.6, No 5 (2013), pp 97-116.
- [12] Singla A, Sachdeva R. Review on Security Issues and Attacks in Wireless Sensor Networks. *International Journal of Advanced Research in Computer Science and Software Engineering*, ISSN: 2277-128X , Vol.3, Issue 4, April 2013.