International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 5, May 2014

Security Protocols against the Network Attacks On Wireless Sensor Network

[1]Soni Panwar, [2]Rupali Rohankar

[1, 2]Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University, Noida , India

Abstract: ***Wireless Sensor Network is a mostly used technology of today world. So lots of attack also occurs on wireless sensor networks when user uses the networks. This paper considers the attacks and provides the countermeasures solutions against the attacks.***

Keywords: Wireless Sensor Networks, Security, Solutions

1. Introduction

In this paper, I consider the different attacks of wireless sensor networks at network layer such as Sybil attack, sinkhole attack, spoofed or altered attack, Hello flood attack, acknowledgement spoofing and so on and find their solutions on respective attacks.

2. Background

On wireless sensor networks, there are different types of attacks on network layer are as following:

- Spoofed or Altered Attack.
- Sinkhole Attack.
- Sybil Attack.
- Acknowledgement Spoofing.
- Hello flood Attack.

Tampering and jamming types of attacks are handled on Physical layer [1]. For control the Physical layer attacks, user use encryption techniques, so attacker cannot modified the contents of the message. For this we used cryptographic techniques. Misbehavior detection and identity protection are done on MAC Layer [1]. In network layer main issues are locating the destination node and calculating the optimal path from source to sink node. SPINS to be the first security architecture designed [9]. It is consist of two secure building blocks: SNEP and µTesla. SNEP offer data confidentiality, data freshness, integrity and two part data authentication. SNEP stands for Sensor Network Encryption Protocol. It was designed to enable data centric information dissemination in sensor networks. SNEP uses a shared counter between sender and receiver so it creates lower communication overhead. SNEP uses message authentication (MAC) to achieve data authentication and prohibits the retransmission of message block with the help of counter. SPINS solve the resource blindness problem by naming the data so sensors request only those resources in which sensor is interested and sensor make decisions on the basis of available resources. µtesla(Micro version of Timid Efficient Stream Loss-tolerant Authentication) provides authentication for data broadcast. µTESLA introduce asymmetry through a delayed disclosure of symmetric keys, its lead to efficient broadcasting, it requires base station and the sensor nodes should be loosely synchronized. Its addition, each node must know the upper bound of error in synchronization. SPINS assume at the time of creation, each node is pre-distributed with a master key that is shared with the base station.

If A wants to send a message to base station B, the complete message A sends to B is:

A _ B: D<KencrC>, MAC(Kmac, C | D) <KencrC>

Where
a key Kencr for encryption,
a key Kmac for MAC generation,
a key Krand for random number generation ,
D is the transmitted data and

C is a shared counter between the sender and the receiver for the block cipher in counter mode. The counter C is incremented after each message is sent and received in both the sender and the receiver side.

SPINS limit the broadcasting capability to the only base station. This limitation overcomes by LEAP.

TINYSEC:
Karlof et all(2004) designed the replacement for the unfinished SNEP known as TinySec. It provides access control, integrity, authentication and confidentiality through encryption. TinySec allow two varients, TinySec-Auth and TinySec-AE. TinySec-Auth provides only for authentication and entire packet is authenticated using a MAC and TinySec-AE provides for encryption and authentication, it encrypt the payload and authenticated the packet using MAC.

INSENS:
Intrusion Tolerant Routing Protocol for Wireless Sensor Network (INSENS) proposed by Deng et al that adopts a routing based approach to secure WSNs [10]. It construct route table of each node. This protocol not completely controls the attacks but reduce the damage of the attacks. It uses multipath routing so message can reach to the destination without passing the malicious nodes.

INSENS have two phases:

i. Route discovery
ii. Data Forwarding

i. In route discovery phase , base station sends the message to all the nodes by using multi-hop

forwarding. If any nodes receiving the request of the record of the sender id, send the message to all its immediate neighbors if nodes already not receive the message. Base station calculates the forwarding table for all nodes with independent two paths. Repeated flooding is not allowed in this process.

ii. In data forwarding phase, data forwarding take place on the basis of forwarding table.

TRANS:
Trust Routing for Location Aware Sensor Network (TRANS) proposed by Tanachaiwiwat et al. It is used in data centric network. To ensure message confidentiality, it uses loose time synchronization asymmetric cryptographic technique.

3. Routing Protocols

Functionality of the network layer is to provide routing, there lots of challenges in the routing due to power saving, sensor nodes have limited power and nodes need to be self organized. Routing protocols are designed to provide a secure route to travel the packets through the network. This security routing protocols are divided into three sections:

Flat routing protocols:

In flat routing protocols all nodes have equal functionality [6]. Example of flat routing protocol is direct diffusion.

Hierarchal routing protocols:

In this different nodes have different roles. These protocols can be event driven, time driven and query driven. Examples are LEACH (The Low-Energy Adaptive Clustering Hierarchy), GAF, SPAN,, PEAS (Probing Environment and Adaptive Sleeping), CLD (Controlled Layer Protocol)and MTE (Minimum Transmission Energy) .All protocols solve the routing and energy problem using clustering and distributing technique.

Time driven protocol if continuous then they are periodic. In the case of even driven, sensor nodes respond according to the action and sensor respond on the basis of query in query driven.

Location based routing protocols: In this technique, location of nodes is used to route the data through the network.

4. Security Mechanism

Security mechanism of wireless sensor network such as key establishment, secure localization, and secure aggregation and security protocols also designed to provide security against the attacks.

Cryptography: Its aim to hidden the main content of the message. Cryptography technique use encryption method to encrypt the packet or decryption method to decrypt the packet in the network

Symmetric: Symmetric Cryptography mechanism means sender and receiver shared a secret key to encrypt and decrypt the message. Most WSNs use symmetric cryptography due to limited hardware and small energy devices.

Two types of symmetric ciphers are: Block ciphers and Stream Ciphers.

Block ciphers work on the blocks of a specific length of data and stream Ciphers works on bitwise of data.

Challenge in symmetric cryptography is how to securely distribute the shared keys between the sender and receiver. Five popular schemes are RC4, RC5, IDEA, SHA-1 and MD5.

Public key cryptographic keys algorithms used in wsn are Diffie-Hellman Key agreement protocols and RSA signatures. Public cryptographic such as RSA takes more communication time which expose the vulnerability to DOS attacks by Brown et al. and take more energy than symmetric cryptography. The implementation of ECC and RSA on Mica motes make it viable to WSNs. But secure peer to peer data authentication and secure data aggregation is not available under public keys these services available under private keys.

Asymmetric: In this technique, we use both keys public and private keys. Sender send the message using public key but receiver can only decrypt the message using private key. ECC is an asymmetric algorithm.

Hybrid: Hybrid Cryptographic techniques include symmetric and asymmetric cryptography algorithms such as AES is better symmetric cryptography technique and ECC (Elliptic Curve Cryptography) is better asymmetric cryptographic technique for WSN

Steganography: Its aim to hidden the existence of the message. Steganography is the art to covert communication by embedding message into multimedia data.

Security requires:

1. Full fill the security principles. These security principles are authentication, confidentiality, integrity, Freshness, self organization. Secure localization and time synchronization to secure the network.
2. Establish the keys in the network using symmetric technique and asymmetric technique.
3. Secure routing

    1) Security Manager
    2) Security Manager

It WAS by Heo and Hong to gives a method to authenticated key agreement []. It depends on elliptic curve cryptography and public key infrastructure. It provides specific domain parameters. Devices use the parameters those provided by security manager to secure the data in the network.

5. Key Management Protocols

Key management protocols: Key management is a main security mechanism in network in WSNs. Goal and public is

to establish the keys between the nodes in secure and reliable manner. Since nodes in WSNs are energy and resource constraint, so key management protocols must be extremely light weight. Key management protocols can be used based on the network structure and the probability of keying. On the basis of network structure, key management protocols can be centralized or distributed. In centralized there is only one entity that generate, regenerate and distributes the keys. This entity called KDC (Key distribution Centre). Only centralized key distribution existing is LKHW scheme. LKHW based on logical key hierarchy. Base station act as KDC and all keys are logically distributed in a tree rotted as a base station. The main disadvantage if centralized controller is failure all security collapse. There is no data authentication and lack of scalability. In distributed key management, there are different distributed controllers they can manage different key activities and there is no problem of single point failure and no issue of scalability. Most of the existing key management protocols are distributed in nature.

On the basis of key sharing:

Key sharing can be Deterministic and Probabilistic.

Deterministic key distribution Scheme:

LEAP:
Zhu et al. proposed the Localized Encryption and Authentication Protocol (LEAP) as a key management protocol for sensor based on symmetric key algorithms [8].

Depend on the security requirements; it uses different keying mechanism for different packets .Four types of keys are established for each node:

1) An individual key shared with the base station.
2) A group of keys shared by all the nodes in the network.
3) Pair-wise key shared with immediate nodes.
4) Cluster keys shared with multiple nodes.

BROSK:
Broadcast Session Key Negotiation Protocol (BROSK) was proposed by Lai et al. BROSK assumes master key shared by all the nodes in the network. BROSK is scalable and energy efficient.

Combinatorial theories:

A Combinatorial theory proposed by Camete and Yener . The combinatorial design theory based on pair wise key pre-distribution (CDTKeying) scheme is based on block design techniques in combinatorics. It employs symmetric and generalized quadrangle design techniques. Lee and Stinson proposed two combinatorial design theories based deterministic schemes: ID-based one-way function scheme (IOS) and deterministic multiple space blooms scheme (DMBS).

PIKE:
Peer Intermediaries for Key Establishment (PIKE) was proposed by Chang and Perrig to established keys between every pairs of neighboring nodes in WSNs. Probabilistic Key Distribution Schemes:

Eschenauer and Gligor proposed a random key pre-distribution scheme for WSNs that relies on probabilistic key sharing between the nodes of a graph in WSNs.

This mechanism has three phases:

1. Key pre-distribution,
2. Shared key discovery
3. Path Key establishment

(i) In Key pre-distribution phase, equipped with the key ring, key ring stored in its memory. The Key rings consist of randomly drawn k-keys from a large pool of keys. Each sensor node shared a pair-wise key with the base station. Association information of key identifier in the key ring and sensor identifier is also stored in the base station.

(ii) In shared key discovery phase, each sensor discovers its neighbors with shared keys.

(iii) In path key established phase, a path key is assigned for the sensor nodes which come within the communication range.

6. Solutions

In Sinkhole attack, an adversary's aim is to attract all the traffic of the network that is destined to the sink by attracting the surrounding node with the help of advertising the high quality route through the compromised node. Through this advertisement, each neighboring node forward the packets through the compromised node intended to sink.

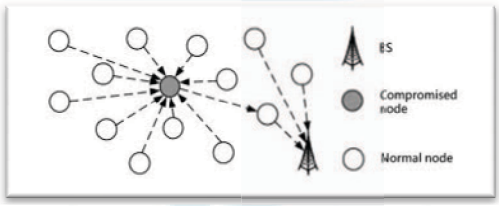

Figure 1: Sinkhole attack

Solutions apply to secure the network against the sinkhole attacks are:

Node validation is a defensive method against the sinkhole attack. Before accepting a node in the network, a node should be authenticated .In this method, sink use a valid key to validate the node.

Selective forwarding:

In selective forwarding attack, an attacker introduce malicious node which send only selective information and drop other information. These malicious node may not forward certain messages simply drop them.

Selective Forwarding considers two cases:

Case 1: Message Selective Forwarding: The attacker sends the information to the particular sensor.

International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 5, May 2014

Case 2: Sensor Selective Forwarding: The attacker sends the information from the particular sensor.

Counter Measures against the Selective forwarding attack:

Using Observer nodes:

Some observer nodes are implemented in the network which assures that neighboring nodes send the received messages.

Using Watchdog and listening to the channel:

In watchdog technique, we observe the network whether a supervising node received the sending message or not. In Listening to the channel, we listen the channels each node should send the same message further to their neighboring node.

Multi Step routing:

Uses multiple paths to send the message throughout the WSNs network.

Using encoding the data:

Use Cryptographic techniques to encrypt the message at sender end and to decrypt the message in receiver end in the WSNs.

Sybil attack:

In Sybil attack, a node forges the identity of more than one node. Sybil attack tries to degrade the integrity the data, resource utilization that the distributed the algorithm to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation. Any peer to peer network is vulnerable to Sybil attack [8].

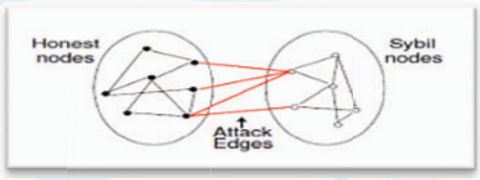

Figure 2: Sybil attack

Defense Measure:

Random Key pre-distribution technique:

- A random generated set of keys is assigned to each sensor nodes, so in key set phase , each node can discover common keys share within the neighboring nodes.
- Identity of each node associated with the associated keys of the node.
- The common keys can consider as secret keys between the neighbors nodes to ensue secrecy between the nodes to node.

Acknowledgement Spoofing attack:

This attack is launched when attacker attempts to encourage the node to transmit the packets at weak links. This can be achieved by convincing that the weak links are strong by spoofing acknowledgments for overheard packets those destined to neighboring nodes.

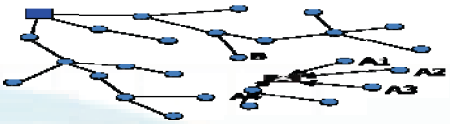

Figure 3: Acknowledgement spoofing

Defense Measure against acknowledgement spoofing:

Append the MAC:
Add the message authentication code at the sending time and the receiving end receiver receives the MAC and verify the packet received.

Wormhole attack:

Wormhole attack is a significant threat to wireless sensor networks, because, this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover neighboring information. In this attack, malicious nodes can eavesdrops on the series of packets in the network and tunnel them into the network and can replay them.

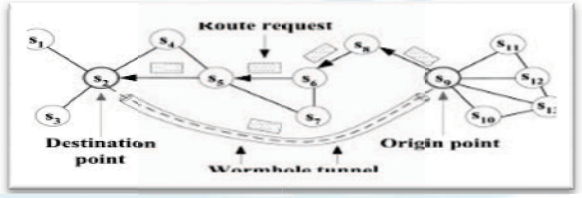

Figure 4: Wormhole attack

Counter Measure against the Wormhole attacks:

Packet Leashes: It is used to detect the attack and then defend against the attack.
Directional antenna: By employing directional antenna, we can defend the wormhole attack, Key Establishment and Broadcast authentication.

HELLO flood attack:
The Hello flood attacks can be caused by a node which broadcasts a Hello packet with very high power, so that a large number of nodes even far away in the network choose it as the parent . All messages now need to be routed multi-hop to this parent, which increases delay.

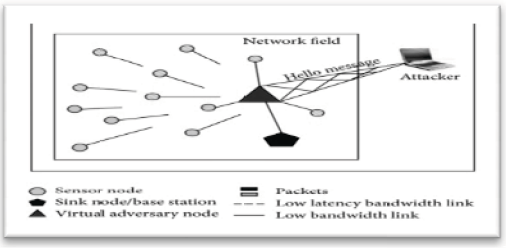

Figure 5: Helloflood Attack

Counter measure against Hello Flood attack can be avoided by the verification of the bidirectional link of the network.

7. Conclusion

In Wireless Sensor Network, there are different obstacles to use this technology such as limited power, limited storage and unattended operations to monitor in remote areas and due to the connectionless nature, it is also not secured. To secured this technologies different cryptographic algorithms are applied to secure the data travelling in the network and different efficient routing protocols to secure the route of the packets in the network. Wireless Sensor network can be more secure if we secure the localization of the sensor nodes and aggregate the data with the help of good aggregation algorithms. If we combine the aggregation and good routing protocols then we can more secure the network and provide more security to wireless sensor network.

References

[1] Manju V.C.," A Survey of Wireless Sensor Networks Journal of Engineering and Innovative technology, August 2012.
[2] Atul Yadav, Mangesh Gosavi , Parag Joshi, "Study of Network Layer attacks and counter measures in Wireless Sensor Network" International Journal of Computer Science and Network, august2012.
[3] Mark A. Perillo and Wendi B. Heinzelman," Wireless Sensor Network Protocols".
[4] Jalil Jabari Lotf, Seyed Hossein HosseiniNazhad ghazani," Security and Common Attacks against Network Layer in Wireless Sensor Networks", Journal of Basic and Applied Scientific Research, 2012.
[5] S.A. Cametepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks", In Proceedings of the 9th European Symposium on Research Computer Security, 2004.
[6] Lee and D.R. Stinson, "Deterministic key pre-distribution schemes for distributed sensor networks", In Proceedings of Selected Areas in Cryptography, 2004, pp. 294-307.
[7] J. Lee and D.R. Stinson, "A combinatorial approach to key pre-distribution for distributed sensor networks", In Proceedings of the IEEE Wireless Communications and Networking Conference.
[8] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanism for large scale distributed sensor networks", ACM Conference on Computer and Communications Security, 2003, ACM Press.
[9] A. Perrig, R. Szewczyk, V. Wen, D.E. Culler, and J.D. Tygar, "SPINS: Security protocols for sensor networks", Wireless Networks, Vol.8, September 2000.
[10] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing in wireless sensor networks", Department of Computer Science, November 2002.
[11] J.N. Al-Karaki and A.E. Kamal, "Routing techniques in wireless sensor networks: A survey, IEEE Wireless Communications, December 2004.
[12] W. Du, R. Wang, and P. Ning, "An efficient scheme for authenticating public keys in sensor networks", ACM International Symposium on Mobile Ad hoc Networking and Computing, New York, ACM Press, 2005.
[13] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses", 3rd International Symposium on information Processing in Sensor Networks, ACM Press 2004.
[14] Karlof, C., Wagner, D (2003) "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Ad-Hoc Networks 1(3), 293-315.
[15] Sarma, H., Kar, A. (2006) 'Security Threats in Wireless Sensor Networks', 2006 International Carnahan Conference on Security Technology, 16th-20th October 2006, Kentucky, USA.
[16] David Boyle, Thomas Newe,"Securing Wireless Sensor Networks: Security Architectures, Journal of Networks, VOL 3, 2008.

Author Profile

Soni Panwar did B. Tech in CSE branch from U.P.T.U. University in 2011 and persuing M. Tech. in CSE branch from Amity School of Engineering and Technology, Amity University, Noida Campus.

Rupali Rohankar pursuing PHD from JNU University, Delhi and currently work as a assistant professor in Computer science department in Amity School of Engineering and Technology, Amity University, Noida Campus.