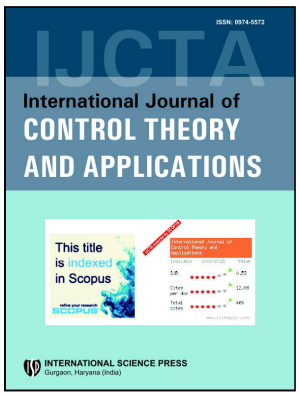

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 15 • 2017

Study of Attacks & Countermeasures on Layers of Wireless Sensor Networks

Sachin Lalar[1], Surender Jangra[2] and Shashi Bhushan[3]

[1] *Ph.D Research Scholar, Department of Computer Science & Engineering* IKGPTU, Kapurthala, Jalandhar, Punjab, India, *Email: sachin509@gmail.com*
[2] *Department of Computer Applications* Guru Tegh Bahadur College, Bhawanigarh, Sangrur, Punjab, India, *Email: jangra.surender@gmail.com*
[3] *Professor, Department of Information Technology CGC, Landran, Punjab, India, Email: shashibhushan6@gmail.com*

Abstract: Wireless Sensor Networks (WSNs) are quickly growing as a significant aspect in wireless and mobile computing research. WSN are usually characterized by limited power/energy, little memory size, low transfer speed. Sensor network used the radio frequency communication for transfer of data between nodes. During the communication, different attacks can be possible on the data. Hence, Security is a great challenge for Wireless sensor networks due to the limited resources. Security mechanism is required to function in wicked environment. The main purpose of this paper is describes the different type of layer attacks on WSNs. It covers the different attacks based on layer of WSNs followed by its probable countermeasures.

Keywords: Wireless Sensor Network, Attacks, Countermeasures

1. INTRODUCTION

Wireless Sensor Networks (WSNs) is rapidly growing because it provides the alternative to solve a great variety of real-world problems. WSN consists of spatially distributed autonomous sensors. Sensor networks are having nodes which equipped with a tiny micro controller, a radio receiver and energy source typically a battery. The applications of WSN are area monitoring, process management, health care monitoring, water quality monitoring etc.WSN are usually characterized by restricted power supplies, small memory size, low transfer speed and limited energy WSN are having the limited resources, mainly memory size and power source. Limited resources represent the obstacles in implementation of traditional security techniques. During the communication, it is easy to eavesdrop, intercept, inject and modify transmitted data. Therefore security of this broadcast communication is having importance and one of the complicated problems to resolve. [1] [2]

The main purpose of this paper to describe the different type of layer attacks on WSNs with probable countermeasures. The paper has 7 sections which are divided as: Section 2 presents the layer architecture of

sensor network; Section 3 to Section 7 describes the different type of attacks based on layer of WSNs with its probable countermeasures and finally conclusion is drawn.

2. LAYER ARCHITECTURE OF WSN

Wireless Sensor network have five different layers as described below:-

- Physical layer: The Physical layer addresses the issues of Selection of frequency, modulation, signal detection, data encryption and carrier frequency generation.
- Data link layer: The main operation of this layer is detection of data frame, access of medium, error control and multiplexing of data streams.
- Network layer: This layer allocates the address and in charge for routing of packets.
- Transport layer: This layer performs the transport of reliable and trusted packets.
- Application layer: It is mainly used for management and processing of the data with the help of different application software. [3]

In Wireless Sensor Network, different type of networks can be possible. The next sections describe the attacks with their solutions on the layers of WSN.

3. PHYSICAL LAYER ATTACK

At the Physical layer, the following attacks are possible:-

3.1. Device Tampering

- The least difficult approach is to break or change sensors physically and therefore avoid or modify their services. The effect will be bigger if base stations are targeted as the base stations are having more data for processing than normal sensors.
- Another way to deal with this attack is to take hold of sensors and pull out the important data from them. With this information, more attacks are possible.
- Device Tempering are frequently characterized in following types: invasive attacks which involve for accessing the hardware such as chips and also require high technology devices, and non-intrusive that require reduced amount of time and extra versatile.
- JTAC1 Attack: The attacker takes the control on the sensor node by testing access port (TAP).
- Misusing the Bootstrap Loader (BSL): By exploiting the BSL, Attacker can access the micro controller's memory. Attacker can read the EEPROM where important data are stored.
- The effects of device Tempering can disturb the entire network service.[4]

3.1.1. Countermeasures

- The common technique to appreciate this attack is to disconnect the link between memory chips and the micro controller.
- Chakib given the key management protocol that detects the inoculation of malicious nodes. [24]
- Common protections can also be applied such as disabling the JTAG interface or by setting the high quality password of bootstrap loader.

3.2. Eavesdropping

- Throughout communication, data in form of signals are travelled in the air and therefore accessible to all. Eavesdropping attackers observe the communication channels without senders and receivers' knowledge and gather the data. .
- The potential of this attack relies on upon the ability of antennas. The weaker signals can be received by attacker if antenna is powerful.
- These types of attack are difficult to detect as it is of passive behavior.

3.2.1. Countermeasures

- Access Restriction
  - A couple of methods exist these days that keep aggressors from getting to the remote medium being used and spread spectrum communication. [5]
  - By restricting the way of the signal propagation, it decreases the possibility of getting access to the communication channel.
- Encryption

3.3. Jamming

- It disrupts the accessibility of transmission media. These methodologies introduce the strong interference to block the channel and dispossess ordinary sensors of the opportunities to convey.
- Foes can disturb a whole sensor system by deploying adequate number of jamming devices.
- Jamming can disrupt the network communication.
- Different jamming strategies as constant jamming, misleading jamming, random jamming & reactive jamming can be used by attacker.[6]

3.3.1. Countermeasures

- Frequency-Hopping Spread Spectrum (FHSS) which incorporates switching so as to send information quickly on carrier sense amongst the frequency channels/ code spreading.
- Sensor Nodes can attempt to map out the jammed area by separating the contaminated region.
- Channel surfing method is also a solution of this attack. [7]

4. MAC LAYER ATTACK

The following type of attack can be possible on MAC layer as:-

4.1. Traffic Manipulation

- The transmission in WSNs can be often effectively control in MAC layer. Foe can broadcast the packets at the same time when legitimate users also transmitting the data, therefore the collision of packet will be occurred.
- The timing of packet can be easily calculated to observe the transmission media and performing a little estimation on MAC layer protocols.

- The collisions not only degraded the network performance but also reduce the signal quality and network availability.

4.1.1. Countermeasures

- "Watchdog" can be used to monitor every node.
- Reputation mechanism can be used to distinguish among the nodes i.e. bad, good nodes.
- Back-off values can be used by receiver and assign a value to each sender. When receiver detects the misbehavior of sender, the receiver will add some more value in corresponding sender back-off value.

4.2. Identity Spoofing

- MAC identity of a sensor node can be easily available to all node including attackers.
- With this information, attacker can replicate that identity and profess to be an alternate one.
- These types of attacks are the base of further attacks such as Sybil attacks which can interpretation the information or give wrong data to router to dispatch false routing attacks.

4.2.1. Countermeasures

To prevent the identity spoofing, the following solution is possible:

- Cryptography-based authentication
- False Identify Detection
- Position verification
- Sequence checking
- Identity-key association

4.3. Collisions Attack

- A collision is the point at which more than one node forward the packet at the same recurrence and at the same information rate.
- Foe can broadcast the packets at the same time when legitimate users also transmitting the data, therefore the collision occurred.[8]

4.3.1. Countermeasures

- Jamming countermeasures can be used.
- Error correcting codes can be used for avoiding the collision.

4.4. Exhaustion Attack

- Exhaustion attack consume all the resources energy of the victim node, by obliging it to do calculations or to receive or transmit unnecessarily data

4.4.1. Countermeasures

- By Limiting the MAC confirmation control rate.

- Different technique, Rate Limiting and Time Division Multiplexing, can be used for protect from this attack.

5. NETWORK LAYER ATTACK

Network layer finds the destinations and computing the ideal way to a destination. The attacks that can be possible in this layer are described below:

5.1. False Routing

As the name proposes, false enforcing so as to direct attacks is dispatched by false routing data. There are three diverse methodologies of authorization:

- Overflowing routing tables
- Poisoning routing tables
- Poisoning routing caches

5.1.1. Countermeasures

- Use of authentication methods
  - Link-level authentication mechanism
  - Hop-to-hop authentication

5.2. Packet Replication

- Attackers retransmit the packets earlier got from other nodes.
- Flooding of this packet can be made to the entire network or to specific nodes.
- So large number of packet is replayed by that the bandwidth and node 'power are consumed, which prompts early end of network operations.

5.2.1. Countermeasures

- Misbehavior Detection technique can protect from this attack.
- Watchdog or IDS can reduce the effect of this attack.
- Reputation can be checked that depend on nodes are giving the right routing information or not.[23]

5.3. Black Hole

- The attacker does not forward each message he gets, generally known as black hole attack.
- By declining to forward any message attacker gets, the throughput of nodes, particularly the neighboring nodes in range of attacker, is significantly diminished.
- If the locations of the attacker near the base station then the throughput of the network is significantly reduced.

5.3.1. Countermeasures

- Use of cryptographic technique with keys can reduce the impact of this attack.
- Received Signal Strength Indicator (RSSI) can be used for readings the messages.[24]

5.4. SinkhHole

- Having certain information of the directing convention being used, foe tries to pull in the activity from a specific district through it. For instance, foe can report a false ideal way by publicizing alluring force, data transmission, or top notch courses to a specific locale.
- Another nodes will believe the way through this attacker node superior to the as of now utilized one, and move their activity onto it. Since influenced nodes rely on upon the attacker for their correspondence, the sinkhole assault can make different assaults proficient by situating the attacker in occupied data activity. [9]
- Many different assaults, for example, spying, specific sending and black holes, and so on, can be enabled by sinkhole attacks.

5.4.1. Countermeasures

- Use of cryptographic technique with keys can diminish the impact of this assault.
- Received Signal Strength Indicator can be used to prevent from this attack.
- Mobile agent scheme can be used against this attack. [10]

5.5. Selective Forwarding

- The foe specifically sends the data of a specific sensor. Foe sends/disposes of the data from chosen sensors. It is considered as in the network layer and is the center of this subsection.
- It will occur only where foe is in the way between paths of data transfer in a multi-hop network.
- It have to put himself in the routing path with help of different attacks like Sybil, sinkhole and routing table poisoning attack. [11]

5.5.1. Countermeasures

- Use a quintessential scheme.
- End-to-End Acknowledgements can increase the quality of route.
- Cryptographic method can reduce the effect of these attacks.[12] [13][14]

5.6. Wormhole

- A wormhole attack need those foes having enhanced communication sources than common nodes and set up good communication way between them.
- Sensors try to transfer the data on communication channel which provide their output to the attackers.

5.6.1. Countermeasures

- This attack can be solved by 4-way handshaking messages.
- Another solution to this attack, all nodes will work with directional antennas.[15][16]
- Packet Leash Method can be used for protecting from wormhole.[17]

5.7. Hello Flood Attack

- To discover the neighbor, HELLO packets is transmitted by nodes.

- In this attack, Attacker floods the HELLO packets to nodes and after that endorse the path to sink.

5.7.1. Countermeasures

- Use of Identity Verification Protocol.[18][19][20]

5.8. Acknowledgement Spoofing Attack

- Acknowledgments are used to persuade whether a delicate connection is well-built or a silence node is active or not.
- Attacker can spoof the acknowledgement & a specific path can be selected by that link look like lost or corrupted.

5.8.1. Countermeasures

- It can be precluded by means of good encryption and authentication methods.
- Different key distribution such as SNEP, TESLA can prevent from this attack. [4]

6. TRANSPORT LAYER ATTACK

Flooding, Injection false message, Energy drain & De-Syn are different type of attacks in the transport layer:

6.1. Flooding

- Attacker node can bring about colossal activity of futile messages on the network cause flooding.
- It reduces the network performance as flooding increase the network congestion.
- Denial-of-service attack is a part of Flooding.

6.1.1. Countermeasures

- At every node end, use of the authentication mechanism to check the validation of message. The authentication mechanism can be used by identity verification through trust based station.
- During the joining of a node to a network a puzzle can be given to a node. After solving the puzzle ode can join the network. This process can put a limit of nodes that can be connected to network.

6.2. Injecting false messages – data integrity attack

- The objectives of this assault are to distort sensor information and by doing as such bargain the victim's exploration
- It disturbs the sensor network routine operation so it will get to be useless.

6.2.1. Countermeasures

- Use the Encryption mechanism
- Introduce the Digital signature

6.3. Energy drain attacks

- As constrained measure of power accessible, foe may utilize the nodes to infuse fictional reports into the network or create large traffic in the network.

- That reports can bring the false alarms that waste the response efforts of node and exhaust the energy of a node.
- It target to degrade the performance of network, to demolish the sensor nodes from the network.

6.3.1. Countermeasures

- To reduce the effect of this attack, fabricated reports should drop from the network as soon possible.

6.4. De-synchronization

- It tries to disturb the current connection.
- An adversary always swindles packets to an end host. This host then needs retransmission of dropped frames and as a consequence the power of nodes is wasted, as a consequence degrading the efficiency of the entire network.

6.4.1. Countermeasures

- Required the authentication mechanisms
- Time synchronization
- Maintain the proper timing.[18][22]

7. TRANSPORT LAYER ATTACK

Attacker knows about the data semantics of this layer, so it may manipulate the information to alter the semantics. By this, fake data are offered to applications and resultant abnormal actions. Application attacks are discussed as:

7.1. Clock Skewing

- The goal of clock Skewing is to desynchronize the sensors. It disseminates the false beacon packet with timing information to those sensors which require the synchronized operations.
- As soon as nodes alter their clocks upon the flawed expertise, resultant node will be desynchronized with the access point.
- Despite the fact that authentic beacon packets can take the node back to synchronization, but nodes will swing in between two states by which node is in unstable state. [19]

7.1.1. Countermeasures

- Misbehavior Detection Techniques

7.2. Selective Message Forwarding

- Attackers used the semantics of the payload of the application layer and pick the packet to forward the established on base of the semantics

7.2.1. Countermeasures

- Data Confidentiality Protection
- Encryption Technique

7.3. Data Aggregation Attack

- As soon as data is accumulated, nodes transmit it to the base stations for further processing.
- Attackers may alter the information to be aggregated and compose the final aggregation outcome computed with the aid of the base stations misrepresented.
- The base stations may encompass an inaccurate perspective of the environment observed by the sensors, and may simply take wrong movement.
- This attack can be very dangerous if that attacked is used with either black hole or sink hole. Resultant no data will be reached to the destination node.
- It required only the network layer knowledge.

7.3.1. Countermeasures

- False Reading Detection
- Outlier Detection Algorithm
- Online deviation detection scheme
- Centralized approach. [20][21]

8. CONCLUSION

Security is an important feature for the deployment of Wireless Sensor Networks. In this paper, a study about existing & potential attacks that can be possible in WSNs is described. The attacks are explained according to layer architecture of WSNs. The paper described the different attacks with their countermeasures on physical layer, data link layer, network layer, transport & application layer of WSNs. The study will hopefully give a better view of attacks in WSNs and come across their way to establish secure designs for these networks.

REFERENCES

[1] I. Akyildiz, S. Weilian,Y. Sankarasubramaniam & E. Cayirci, "A survey on sensor networks",*IEEE Communications Magazine, 40*(8), pp 102-114, 2002

[2] H.C.Chaudhari and L.U. Kadam , "Wireless Sensor Network Security Attack and Challenges", International Journal of Networking, pp-04-16, 2011

[3] D.Carman, P.S. Krus & B.J. Matt, "Constraints and Approaches for Distributed Sensor Network Security",*NAI Labs,Network Associates,2000*

[4] J.Deng, R. Han & S.Mishra, "Countermeasures Against Traffic Analysis in Wireless Sensor Networks",*University of Colorado at Boulder, 2004*

[5] M. Franklin, Z. Galil, andM. Yung, "Eavesdropping games: a graph-theoretic approach to privacy in distributed systems,"*J. ACM*, vol. 47, no. 2, pp. 225–243, 2000.

[6] X.Wenyuan, Ke Ma, W. Trappe, and Yanyong Zhang, "Jamming sensor networks: attack and defense strategies", IEEE 2006.

[7] A.D. Wood, J.A. Stankovic, and S.H. Son,"Jam: a jammed-area mapping service for sensor networks", Real-Time Systems Symposium, RTSS 2003. 24th IEEE, pages 286-297,2003

[8] Dr. Shahriar Mohammadi, Hossein Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensors Network" International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.3, No.1, pg 35-56, 2011.

[9] D.Sheela, K.Naveen and G Mahadevan, "A non cryptographic method of sink hole attack detection in wireless sensor networks", Recent Trends in Information Technology (ICRTIT), 2011

[10] Vinay Soni, Pratik Modi, Vishvash Chaudhri, "Detecting Sinkhole Attack in Wireless Sensor Network" Volume 2, Issue 2, International Journal of Application or Innovation in Engineering & Management (IJAIEM).

[11] Wazir Zada Khan Yang Xiang Mohammed Y Aalsalem, , "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks", International Journal of Computer Network and Information Security (IJCNIS), 2011.

[12] Devu Manikantan Shila, Tricha Anjali, "Defending Selective Forwarding Attacks in WMNs" Electro/Information Technology, 2008.

[13] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, Wang Liangmin, "Lightweight Defense Scheme against Selective Forwarding Attacks in Wireless Sensor Networks", pp.226-232, 2009

[14] Guorui Li, Xiangdong Liu, and Cuirong Wang, "A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks", pp.554-558, 2010

[15] Kashyap Patel , Mrs.T.Manoranjitham, 2013. "Detection of Wormhole Attack In Wireless Sensor Network", India International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 5, 2013.

[16] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks", *Network and Distributed System Security Symposium(NDSS)*, 2004

[17] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defence against Wormhole Attacks in Wireless Networks",INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE, pp. 267-279, 2003

[18] Virendra Pal Singh, Sweta Jain and Jyoti Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks",IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11.

[19] Virendra Pal Singh , Aishwarya S. Anand Ukey , Sweta Jain, "Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 62– No.15

[20] S.Madhavi and K. Duraiswamy, "Flooding Attack Aware Secure AODV", Journal of Computer Science, 2013

[21] J. Douceur,"The Sybil Attack", In Proc. Intl Wkshp on Peer-to-Peer Systems (IPTPS), 2002.

[22] Hang Liu, Hairuo Ma, Magda El Zarki, and Sanjay Gupta, "Error control schemes for networks: An overview. Mobile Networks and Applications" 1997.

[23]] M. J. Freedman and R. Morris Tarzan, "A peer-to-peer anonymizing network layer", Proceedings of the 9th ACM conference on Computer and communications security, 2002

[24] Chakib Bekara and Maryline Laurent-Maknavicius, "A new protocol for securing wireless sensor networks against node replication attacks".,Wireless and Mobile Computing, Networking and Communications, Third IEEE International Conference on, pages 54-59, 8-10 Oct. 2007.