DoS Attacks on different Layers of WSN: A Review

Kanchan Kaushal
CTIEMT
Shahpur
Jalandhar, India

Varsha Sahni
CTIEMT
Shahpur
Jalandhar, India

ABSTRACT
WSNs plays an important role in many of the applications like patient health monitoring, battlefields surveillance, traffic control, environmental observation, home automation and building intrusion surveillance. WSNs are convenient, cost effective, and give ease of integration with other networks and their components. However, wireless technology also produces new threats. Since WSNs communicate by using radio frequencies therefore the risk of interference is more than with wired networks. If the message to be passed is not in an encrypted form, or is encrypted by using a feeble algorithm and the attacker can easily read it, and it is the compromise to the confidentiality. Security objectives include: protecting confidentiality, assuring integrity, providing authentication and supporting availability of the information and information systems. In this paper we describe the types of existing DoS attacks and how existing techniques can be used to prevent or mitigate these attacks in WSNs.

General Terms
WSN Security, DoS Attack, Defenses.

Keywords
Security goals, Security threats, DoS Attack on different layers, prevention of attacks.

1. INTRODUCTION
WSNs consist of multifunction and spatially distributed small sized sensor nodes communicate wirelessly over short distances. The sensor nodes unite distinct properties for sensing the environment, as well as communication among other sensor and data processing. It monitors physical/environmental conditions like sound, temperature, pressure, vibration, humidity, motion or pollutants. WSNs plays an important role in many of the applications like patient health monitoring, battlefields surveillance, traffic control, environmental observation, home automation and building intrusion surveillance. The wireless networking has enhanced efficiency through increased receptiveness to information resources and faster, easier and less expensive network configuration. WSNs are convenient, cost effective, and give ease of integration with other networks and their components. However, wireless technology also produces new attacks. Since WSNs communicate by using radio frequencies therefore the risk of interference is more than with wired networks.

If the message to be passed is not in an encrypted form, or is encrypted by using a feeble algorithm and the attacker can easily read it, and it is the compromise to the confidentiality. Unauthorized captured nodes, access points, unknown stations; spoofed acceptance are some of the problems given in WSN troubleshooting. Moreover, onsite maintenance for remotely deployed sensor nodes is infeasible, thus a thorough consideration of security solutions and troubleshooting tools must be available.

2. SECURITY GOALS IN WSN
Some of the issues related to WSN are: Fault tolerance, scalability, production cost, hardware constraints, sensor network topologies, environment, power consumption and security. Most of the sensor networks are located in a vicious environment with active smart opposition. Therefore security is a critical issue. Some of the security objectives or issues include: protecting confidentiality, assuring integrity, and supporting availability of the information and information systems. These goals are given as:

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

2.2 Authentication
Authentication need to know if the message is from the node it claims to be from. Authentication determines the reliability of message's origin.

2.3 Availability
Availability is to determine if a node has the capability to use the resources and it determines the network's availability for the messages to move on.

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

3. TYPES OF ATTACKS ON WSN
WSNs are vulnerable to security attacks because of the reason that nodes are deployed in a dangerous or hostile environment. Hence they have no physical protection. Attacks can be categorized as active attacks and passive attacks.

3.1 Passive Attacks
The monitoring and listening to the transmission of messages by unauthorized attackers are termed as passive attacks. In this type of attacks, the attacker does not change or modifies the information on the network. It just listen the messages transmitted on the network and does not try to modify of alter the messages transmitted on the network. Some common passive attacks in WSNs are:

- Attacks against privacy
- Traffic Analysis
- Camouflage adversaries

Many attacks against privacy are active in nature. Monitor and eavesdropping is the most common attack to privacy. Attacker can also analyze the traffic silently. Camouflages adversaries can insert their nodes or compromise the existing nodes to hide in the sensor network and then these types of nodes can copy as a genuine node to attack on the packets, then misroute packets, conducting the privacy analysis.

3.2 Active Attacks

The attacks in which the unauthorized attacker monitors the communication channel, listens to the transmission and modifies the data stream in that communication channel are termed as active attacks. Some of the active attacks are:

- Routing attacks in sensor networks
- Denial of service (DoS) attacks
- Node subversion
- Node malfunction
- Node outage
- Physical attacks
- Message corruptions
- False node
- Node replication Attacks
- Passive information gathering
- Spoofed, altered and replayed routing information

4. DOS ATTACKS AND ITS PREVENTION

It happens by the unintended collapse of nodes or malicious action. The simplest DoS attack attempt to drain the resources accessible to the victim node, by sending extra needless packets and thus halts legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's seek to corrupt, deprave, or destroy a network, but also for any event that reduces a network's capability to provide a service. [15] In wireless sensor networks, various types of DoS attacks in different layers can be performed. DoS attacks at physical layer are jamming and tampering, at link layer are collision, unfairness and exhaustion, at network layer attacks are homing, neglect and greed, black holes, misdirection and transport layer is vulnerable to the attack performed by de-synchronization and malicious flooding.

4.1 DoS Attack on Physical Layer

Physical layer is responsible for frequency selection, carrier frequency generation, signal deflection, data modulation and encryption. [5] Physical layer suffers the most damage from

4.1.1 Jamming

Jamming is defined as the act of intentionally directing electromagnetic energy towards a communication system to disrupt or prevent signal transmission.[2] In WSN, the transmission of radio signals that interferes with the radio frequencies being used by the sensor networks, this type of attack is jamming attack.[5] Jamming can be of two types:

- Constant jamming
- Intermittent jamming.

Constant jamming is defined as the complete jamming of the entire network so that no messages are able to send or receive on the network. Whereas intermittent jamming is the type in which messages can be exchanged periodically but not constantly.

4.1.2 Tampering

Giving physical access to the sensor nodes is known as Tampering. These are threats to physical node destruction. Unlike many other attacks, physical attacks destroy sensors permanently. So the loses are irreversible. Adversaries may become successful in compromising some of the legitimate nodes in the network. After compromising a node, adversaries may carry out lots of misleading activities inside the network.

Jamming and tampering attacks can be prevented by using methods like spread lower duty cycle, spectrum, priority messages, region mapping, Tamper proofing, mode change and node hiding.

4.2 DoS Attack on Link Layer

Data link layer is responsible for the multiplexing of data streams, data frame detection, medium access control (MAC), data encryption and error control; as well as ensuring reliable point-to-point and point-to-multipoint connections.[5] Three types of DoS attack on link layer are:

- Collision
- Exhaustion
- Unfairness.

4.2.1 Collision

Attackers intentionally violate the communication protocol and continually transmit messages in attempt to generate collisions.

4.2.2 Exhaustion

Such collisions will require the retransmission of any packets affected by the collision and it will exhaust the sensor network's power by forcing too many retransmissions.

Link layer attacks can be prevented by using error detection code, rate limitation and by dividing the packets into small frames.

4.3 DoS Attack on Network Layer

Network layer is responsible for specifying the assignment of addresses and how packets are forwarded. [5] DoS attacks on network layer are:

- Hello Flood attack
- Head node volunteering
- Black hole attacks
- Sybil attack
- Selective forwarding attack

4.3.1 Hello Flood Attack

In this attack, an attacker sends or replays a routing protocol's HELLO packet from one node to another with more energy. This attack makes use of HELLO packets as a weapon to convince the sensors in WSN. In this type of attack, an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN. The sensors are thus influenced that the adversary is their neighbor. As a result, while sending the information to the Base Station, the victim nodes try to go through the attacker as they know that it is their neighbor and ultimately spoofed by the attacker.[13]

4.3.2 Head Node Volunteering

Nodes cluster use one head node to save power. In head node volunteering, the attacker volunteers to be head node and drops packets. Till now, no method is useful to prevent the Head node volunteering attack on the network layer of WSN.

4.3.3 Black Hole Attack

In this type of attack, some of the malicious nodes in the WSN intentionally advertise zero cost routes through them. Then some routing protocols (e.g., distance vector routing) establish a route to a destination **by** selecting this malicious node as an intermediate node into the routing path; (as they look for low cost link). Also the neighbors of this malicious node select this route and compete for the bandwidth. In this process the neighbors of this malicious node waste their energy and create a hole or partition in the network called a black hole.

To prevent the DoS attack on network layer, there are methods like egress filtering, Authentication, Monitoring, Redundancy, Probing and Packet leashing by using geographic, temporal information and by verifying bidirectional links.

4.4 DoS Attack on Transport Layer

Transport layer is responsible for the reliable transport of packets and data encryption. [5] Two types of attacks on Transport layer are:

- Flooding
- De-synchronization

4.4.1 Flooding

Protocols that maintain state information at either end of the communication are vulnerable to flooding attack. One well-known attack is TCP **SYN** flood attack in which the adversary continuously sends the connection requests and floods the network link at the targeted node.

4.4.2 De-synchronization

By disrupting some of the packets transmitting in between the nodes and by maintaining proper timings, an adversary can make a pair of nodes stuck in synchronization recovery protocol. This compels the nodes to waste their energy.

Transport layer DoS attacks like flooding and de-synchronization can be prevented by using client puzzles and authentication schemes.

4.5 DoS Attack on Application Layer

Application layer is responsible for specifying how the data are requested and provided for both individual sensor nodes and interactions with the end user. [5] Application layer attacks are:

- Attacks by sending large amount of stimuli
- Network programming attack
- Path based DoS

4.5.1 Attacks by sending large amount of stimuli

In this attack, Applications are controlled by stimuli i.e. send alert for motion detection causes large amounts of network traffic.

4.5.2 Network Programming Attack

In this attack, the nodes can be reprogrammed in the field and the attacker attack by sending false program.

4.5.3 Path based DoS

In this attack the attacker forwards packets all the way to base station and it uses network bandwidth, node energy.

4.6 Other Prevention Schemes

Wireless communications are endangered to denial-of-service (DoS) attacks. Organizations can take various actions to mitigate the risk of these involuntary DoS attacks. Careful site contemplate can recognize locations where communication from other devices exist; the results of these contemplation should be used while taking decision where to locate the wireless access points. Regular periodic surveys of wireless networking actions and performance can identify problems; suitable remedial activities may include eviction of the humiliating devices or measures to increase strength of and coverage within the problem area.

5. CONCLUSION

In this paper, we have presented a study of some existing DoS attacks of WSN and their security mechanisms.

Our main concern is about security objectives include: assuring integrity, protecting confidentiality, supporting availability and providing authentication of the information and information systems. The other focus is on DoS attack on different layers of WSN and prevention at those particular layers. The main categories are the introduction to WSN, DoS attacks on different layers of WSN and their security mechanisms. Within each of those categories we have also sub categorized the major topics including Jamming, tampering, flooding, and black hole attack etc. Aim of this paper is to extend both a extensive overview of the preferably broad area of security of wireless sensor network. As wireless sensor networks are growing and becoming more common, we look for the further anticipations of security will be required of these wireless sensor network applications.

6. ACKNOWLEDGMENTS

The authors wish to thank the faculty from the computer science department at CTIEMT, Jalandhar for their continued support and feedback.

7. REFERENCES

[1] Vikash Kumar, Anshu Jain and P N Barwal, "Wireless Sensor Networks: Security Issues, Challenges and Solutions", International Journal of Information & Computation Technology, ISSN 0974-2239 Vol 4, No 8, pp. 859-868, 2014.

[2] Javad Afshar Jahanshahi, Seyed Ali Ghorash, Mohammd Eslami, "Fuzzy C-Means Clustering-Based Jamming Detection Algorithm at Base Station", Research Article - Electrical Engineering, Arabian Journal for Science and Engineering, Volume 38, Issue 8, pp 2125-2133, springer, August 2013.

[3] Ahmad Abed, Alhameed Alkhatib, and Gurvinder Singh Baicher "Wireless Sensor Network Architecture," International Conference on Computer Networks and Communication Systems, IPCSIT, vol. 35, 2012.

[4] Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.

[5] Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, And Grammati Pantziou, "A Survey On Jamming Attacks And Countermeasures In Wsns", IEEE Communications Surveys & Tutorials, VOL. 11, No. 4, Fourth Quarter 2009.

[6] Jennifer Yick, Biswanath Mukherjee, and Deepak Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, pp. 2292-2330, Elsevier, April 2008.

[7] Yong Wang, Garhan Attebury, And Byrav Ramamurthy, "A Survey Of Security Issues In Wireless Sensor Networks", IEEE communication surveys, Vol 8, No. 2, 2nd quarter 2008.

[8] K. Kifayat, M. Merabti, Q. Shi, D. Llewellyn-Jones: Group-based secure communication for large scale wireless sensor networks, J. Information Assurance Security. Vol 2, 139–147, 2007.

[9] Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Advanced communication technology, 8th international confference, vol. 2, IEEE, 2006.

[10] T. Roosta, S. Shieh, S. Sastry, "Taxonomy of Security Attacks in Sensor Networks", 1st IEEE Int. Conference on System Integration and Reliability Improvements, , Hanoi (2006) pp. 13–15, 2006..

[11] J. Deng, R. Han, S. Mishra "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks", First IEEE/Cerate Net Conference on Security and Privacy in Communication Networks (SecureComm), Athens (2005) pp. 113–124, 2005.

[12] A. Perrig, J. Newsome, E. Shi, D. Song , "The Sybil Attack in Sensor Networks: Analysis and Defences", 3rd Int. Symposium on Information Processing in Sensor Networks , (ACM Press, New York, USA 2004) pp. 259–268, 2004.

[13] http://www.authorstream.com/Presentation/kudumulavishnu-2146270-security-wireless-sensor-networks

[14] Y.-C. Hu, A. Perrig, D.B. Johnson: Adriane: A Secure On-Demand Routing Protocol for Ad Hoc Networks, Annual ACM Int. Conference on Mobile Computing and Networking (MobiCom) 2002.

[15] K. Gandol, C. Mourtel, F. Olivier, "Electromagnetic Analysis: Concrete Results", Published in C_ .K. Ko_c, D. Naccache, and C. Paar, Eds Cryptographic Hardware and Embedded Systems { CHES 2001, vol. 2162 of Lecture Notes in Computer Science, pp. 251{261, Springer-Verlag, 2001.

[16] Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, "A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks", Journal of Security Engineering.

[17] Anthony D. Wood and John A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", Unpublished.