ANALYSIS OF DENIAL OF SERVICE (DOS) ATTACKS IN WIRELESS SENSOR NETWORKS

Sunil Ghildiyal[1], Amit Kumar Mishra[2], Ashish Gupta[3], Neha Garg[4]

[1]*Uttaranchal University, Dehradun Uttarakhand*
[2]*Uttaranchal University, Dehradun Uttarakhand*
[3]*Dev Bhoomi Inst. of Technology, Dehradun Uttarakhand*
[4]*Graphic Era University, Dehradun Uttarakhand*

Abstract

WSN are made of hundreds of constraints dependent sensors for solving real world sensitive applications. These nodes are scattered over an area to monitor and record the data as desired by the application and to forward same to the center node for further observation, which may generate an alert to control the situation. In recent years, WSN has been grown tremendously in the applications, resulted the demand of a strong, consistent security mechanism. WSN issues, challenges are needed to be addressed for designing such security mechanism. Irrespective of various limited capabilities of nodes, even, on-time collection of information and reliable, secure delivery is expected in WSN. Tiny sensors with small hardware, processing capabilities and limited power resource cannot afford traditional security measures to fight against vulnerabilities. Different layers of WSN nodes have variety of roles to play for proper their proper functioning at different layers like signaling, framing, forwarding, reliable transportation and user interaction at both receiving as well as sending end. Many denial of service attacks are identified at each layer which are meant for purposeful, planned attacks to jeopardize the availability of service, restricting the WSN utility for application. In this paper we will focus on the WSN characteristics, constraints and types of DoS attacks at different layer.

Keywords: *Wireless Sensor Network WSN, Constraints, Threats, Denial of Service DoS, Attack, Vulnerabilities.*

----------***----------

1. INTRODUCTION

Subsequent to the developments in wireless technologies, wireless networks are expected to deliver communication with security requirements like confidentiality, integrity and availability. Firstly, WSN are equipped with low power, low processing capability nodes[1]. Secondly, it is very difficult to enhance the capabilities of these sensors due to their tiny size and hardware constraints. These are important considerations while designing a solution for WSN enabling them to provide above security requirements.

Sensors node use RF for communication with each other hence use broadcast basically. Wireless communication over the broadcast is difficult to protect cause of easy eavesdropping, injecting can be performed over broadcasting. Sensors nodes are scattered over an area physically insecure manner, hence can be stolen, physically tempered easily or after capturing such node physically, any logical security mode can easily be detected or penetrated[2]. Limited resources of the node make it weak and paralyzed in front of any intended flooding attack. Initial measure against such threats is to utilize the sensors for their maximum capabilities to make network fully functional within authorized access and resources.

2. WSN CHARACTERISTICS

The main characteristics of a WSN include: WSN are getting a lot of interest by the researchers, industry due to their less cost solutions to various real world problem solving applications. Other favoring factors of wireless sensor networks are low energy consumption of nodes, portability, unattended operation, ability to withstand bad environmental conditions, having dynamic network topology, to cope with sensor node malfunctioning and failures, Mobility of nodes, Heterogeneity of nodes, Topology and Deployment Scalability, Easy use.

3. WSN CONSTRAINTS

Resource Constraints: Limited processing and very low RF communication bandwidth It is due to their small size and low battery. Computation capabilities are also very low due to less computational capability embedded processor in the hardware.

Memory: There is a flash memory and flash RAM in node. But after loading the OS and application there is no much space for storage. Flash memory is used for storing downloaded application code.

Message size: Message size of WSN is quite small as compared to the any traditional network. It results in no concept of segmentation in WSN applications usually.

No Global addressing: Due to large number of deployed nodes, it is not possible to identify each node with unique addressing at global level.

Location Management: Data is collected by the nodes after they have been deployed at specific place or have been

constant static at same place. Environmental conditions, mobility of nodes may result in difficult location management of nodes.

Data redundancy: Many nodes may record the same physical phenomenon data, may result in high probability of data redundancy.

4. SECURITY REQUIREMENTS IN WSN

The aim of security mechanism is to protect the information from attacks. In wireless sensor networks security requirements make sure that network services are available even in presence of DoS and also in presence on any vulnerability. Only authorized WSN node can be involved in information passing. It also ensures that a malicious node cannot masquerade as trusted node. There has to be confidentiality and integrity in message, what sent from authorized sender to receiver. Data freshness and non-repudiation is also to be taken into account with the security measures, applied or to be. Since the tiny sensor nodes are randomly deployed and operated in unattended environment so the security requirements include self-organization of node which further includes self-configuration, self-management (autonomous) and self-healing (fault tolerant).

5. THREAT MODEL

In WSN, threats are from outside the network and within the network. If attacks are from the nodes of the native network then it is much harmful. Also, it is quite difficult to find out the malicious or compromising node within the native network. Another classification of the attacks may be passive and active where passive attacks don't modify or alter the data as active attacks do. If the opponent attack by using similar capacity nodes for network penetration it is called mote class attack but when powerful devices like laptop are used to penetrate the network then such attack is called laptop attack.

6. ATTACKS ON WSN

The attacks of WSN can be classified into two categories: invasive and non-invasive. Non-invasive attacks generally target to timings, power and frequency of channel. Invasive attacks target to availability of service, transit of information, routing etc. In DoS attack, hacker tries to make service or system inaccessible. However during the transit of information, more common attacks are encountered. Routing attacks are generally inside attacks.

7. DOS AND DOS ATTACKS

There are varieties of DoS conditions. These conditions may temper WSN nodes and network functionality. These may hinder the regular routines of the network, may come up in form of resource exhaustion, any software bug, or any complication while interacting with the application, infrastructure. Any such obstacles in network functionality are called DoS as it affects the availability or fully functionality of service but when it is cause of intentionally by the opponent, these are called DoS attacks.

Dos attack is referred as intended attack of opponent to destroy or destruct the network. DoS attack may limit or eliminate the network functionality than expected. DoS attack may occur any layer of OSI layers of WSN[3].DoS attacks are vulnerable as it penetrates the efficiency of targeted networks by affecting its associated protocols. DoS attacks may consume the resources, destruct or alter the infrastructure configuration and physically destroy the network components.

Wood and Stankovic presented layer wise categorization of DoS attacks first. [4].It was further enhanced by Raymond and Midkiff with some updates [5]. Now we will talk about the DoS attacks at different layers of WSN infrastructure.

8. DOS ATTACK AT PHYSICAL LAYER

8.1 Jamming

In this attack, radio frequencies used by the network nodes are interfered. The adversary can either disrupt entire network or a particular small portion of it. It depends on the power of jamming nodes distributed nearby the network. Jamming is of various types Constant, Deceptive, Random and Reactive[6]. Jamming may be consistent or intermittent. Handling the jamming at MAC layer needs to control the requests which may exhaust the resources by ignoring them. However network layer also deals with jamming by mapping jamming area in the network or in surrounding routing area. If the network is single frequency based, this attack is simple and effective. If the various forms of spread spectrum are used in spectrum, such attacks can be eliminated. Nodes also must have their own strategy to facing such attacks like periodically waking up when jam is ended or low, not communicating with each other or sleep mode during jamming period to conserve the power etc.

8.2 Tempering

In such attack, attacker may physically temper the node and can compromise with them. It is not possible to control hundreds of nodes spread over an area of several kilometers. Attacker may extract the sensitive information like cryptographic keys from node by damaging it to get access to higher level of communication. The only defense mechanism against such attack is temper-proof physical packaging. But it costs additional[7].

9. DOS ATTACK AT LINK LAYER

9.1 Exhaustion (Continuous Channel Access)

In this attack, attacker may disrupt the channel by continuously requesting and transmitting over it. It results in starvation for channel access for other nodes. It is usually done by sending a large numbers of RTS (Request to Send) packets over channel, leading multiple collisions and draining out the nodes of their power. A possible solution for such attack is to limit the request rate so network can ignore excessive requests without sending expensive radio transmissions. This limit cannot drop below the expected maximum data rate the network supports, though. Time

Division Multiplexing is also a technique to prevent such attack as time slots are divided for each node to transmit its contents.

9.2 Collision

Collision occurs when two nodes intend for simultaneous transmission on same frequency channel. If the packets collide, a small change in packet will take place which will be encountered as mismatch at the time of checksum at receiving end and hence packets will be discarded, to be re transmitted. Attackers may need to induce a collision instance in one octet of transmission to disturb entire packet transmission. Even a corrupted ACK message can also induce costly exponential back-off in many MAC schemes. Using error correcting codes is one of the method to prevent such attacks but generally at low level of collisions[8].

9.3 Unfairness

Unfairness is referred as repeated collision based or exhaustion based attacks or an abusive use of cooperative MAC layer priority mechanisms. Also may be called as a weaker form of DoS. This threat may not entirely prevent legitimate access to the access channel but it could degrade service in order to gain an advantage such as causing other nodes in a real-time MAC protocol to miss their transmission deadline.

10. DOS ATTACK AT NETWORK LAYER

10.1 False Routing or Spoofed, Altered, Replayed Routing Information

Such attacks primarily focus on routing protocols mainly for routing information. Nodes exchange routing information at specific time intervals or as per design policy of routing. By changing the routing information by a malicious node, it is possible to change the routing of entire WSN structure or its any network partition. This can be done by altering or changing the routing information, by shortening or extending the route information in the routing table or by generation of false error messages. Strategy against such attack is MAC code implementation along with message. Adding time stamps can prevent against replaying the routing.

10.2 Selective Forwarding

Fundamental principle of WSN is ‘Multi-hop”. It means that sensor nodes will forward the entire message to next node in line what they have received. In this attack, nodes drop few messages instead of forwarding everything of what they have received. Attacking nodes deny routing some messages and drop them. If all the packets are denied for forwarding by anode after receiving, is called black hole attack. In selective forwarding few messages are dropped and few are forwarded further to the next node. One of the defense mechanism against this attack is multiple paths to send the data.

10.3 Sinkhole Attacks

In this attack attackers seem to be more attractive to its surrounding nodes by forging the routing information. Main aim of attacker is to tempt all the nodes in close proximity, constructive a figurative sinkhole. It results in the malicious node to be most chosen for data forwarding through it by other surrounding nodes. These attacks make selective forwarding very simple as traffic from very large surrounding area will flow through the adversary node.

10.4 Sybil Attack

In this attacker attacks a single node in the network with a malevolent code masked with multiple identities. Then this node behaves as polymorphic. Its multiple identities mislead to all other nodes. Some of such identities are decreasing topology maintenance schemes, disparity in storage, disparity in routing. This attack includes a major concern for Geographical Routing Algorithms which needs the location of a node to route the message efficiently.

10.5 Wormhole

Wormhole is referred as low latency link between two portions of a WSN network over which an attacker replays network messages [9]. Here an adversary convinces the nodes which are multi hop away that they are closer to the base station (BS) The wormhole attack usually engage two different and far away malevolent codes conspire to minimize their remoteness from each other by replaying packets next to an out-of-reach channel, is only available to attacker.

10.6 Hello Flood

Malicious nodes sometime can cause of immense traffic of useless messages. It is known as flooding. Malicious nodes, sometime replay some broadcast traffic which is useless but congest the channel. In hello flood type attack, attackers use very high power RF transmitters to handle the large area of nodes into trusting that they are neighbors of it. Attacker will broadcast a false superior route so that other nodes will attempt very far from it in RF distance.

10.7 Acknowledgment Spoofing

Many routing algorithms used for WSNs require transmission of acknowledgment packets from receiver to sender as a token of successful receipt. Attacking node may spoof the acknowledgements of overheard packet destined for neighboring nodes in order to provide false information to those nodes.

11. DOS ATTACK AT TRANSPORT LAYER

11.1 Flooding

Any protocol which maintain state at either end, it has to face a problem called flooding[10].Attacker may repeatedly establish new connection requests until the resources are exhausted, which were required by each connections or reached maximum limit. Under such conditions, further

legitimate requests will be ignored. Limiting the number of connections prevents from complete resource exhaustion. One of the possible solutions of this problem is to require that each connecting client demonstrate its commitment to the connection by puzzle solving.

11.2 De-Synchronization

Connection between two endpoints can be disrupted by de-synchronization. In this attack, the adversary repeatedly forges messages to either or both endpoints. For example, there may be requests for retransmissions of missed frames by the repeated spoof messages. If timed correctly, an attacker may degrade the functionality, capability of end hosts by retransmission of frames unnecessarily. It causes endpoints to waste the energy for attempt to recover from errors which never really exist. One possible solution to this problem is authentication of all packets exchanged, including all control fields in the transport protocol header. There are many algorithms designed to overcome this attack in single-hop as well as multi-hop environment.

12. DOS ATTACKS AT APPLICATION LAYER

12.1 Path Based Dos

It is a kind of attack of attack where number of nodes which are present in the path from source to the base station towards the forwarding information, are drained by the number of bogus packets, sent to the path towards base station[10]. Under such conditions node becomes busy and it denies for legitimate traffic transmission. Use of effective authentication mechanism may prevent from such type of attacks[11].

12.2 Reprogramming

There is a need of reprogramming in WSN for version control, code acquisition, encoding-decoding, its infrastructure management or to switching to new program. If this reprogramming schedule is not secured, attackers may easily can get access and can actively cut off a portion of the network by use of bogus messages. A good authentication mechanism can prevent from such attacks[12].

13. CONCLUSIONS

There are many other attacks also which can obstacle the smooth functioning of wireless sensor networks like denial of sleep, Homing etc. Under many circumstances, attacks may overlap also with each other. At physical layer attacks and their measures are important issues as these attacks are much difficult to handle. Sensors have native radios of very low power and are operated in unattended environment, hence are not capable of resisting such attacks. Though there are many algorithms and mechanisms for network security and also to prevent from above mentioned attacks but those are of no use for WSN due to their constraints as mentioned above. However there are many tiny low computational algorithms available for WSN and being applied also. But they have not been proved as precise measures against above attacks. Any DoS situation in WSN either intentionally or unintentionally needs to be addressed by strong mechanism. DoS attack includes a large variety of attacks, sometime altogether. It is always advisable to develop and deploy a proper suitable measure in WSN as prevention already.

REFERENCES

[1] Doddapaneni.krishna chaitanya "Analysis of Denial-of-Service attacks on WSN using simulation" Middlesex University.

[2] Ritu sharma, Yogesh Chaba, Yudhvir Singh "Analysis of security protocols in wireless sensor networks" Int. Journal Advanced Networking and Applications Vol 02, Issue 03.

[3] Al-sakib Khan Pathan "Denial of Service in Wireless sensor networks: issues and challenges**."**Advances in communications and Media Research ISBN 978-1-60876-576-8.

[4] Wood, A. D. and Stankovic, J.A. (2002) " Denial of Service in Sensor Networks" IEEE Computer, vol. 35, no. 10, 2002, pp 54–62.

[5] Raymond, D. R. and Midkiff, S. F. (2008) "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses" IEEE Pervasive Computing, January-March 2008, pp 74-81.

[6] Xu, W., Trappe, W., Zhang, Y., and Wood, T. "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks' ACM MobiHoc'05, May 25–27, 2005, Urbana-Champaign, Illinois, USA, pp 46-57.

[7] Anthony D. Wood, John A. Stankovic " Denial of Service in Sensor networks" University of Virginia 0018-9162/02/$17.00 ©2002 IEEE

[8] Mohit Saxena " Security in Wireless Sensor Networks A Layer based classifications" Purdue University, West Lafayette IN 47907

[9] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.

[10] A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", *IEEE Computer,* Vol. 35, No. 10, pp. 54-62, 2002.

[11] Deng, J., Han, R., and Mishra " Defending against Path-based DoS Attacks in Wireless Sensor Networks" ACM SASN'05, November 7, 2005, Alexandria, Virginia, USA., pp 89-96.

[12] Wang, Q., Zhu, Y. "Reprogramming Wireless Sensor Networks: Challenges and Approaches" IEEE Network, May/June 2006.