Active Denial-of-Service Attacks in Wireless Sensor Networks

Shobhit Gupta
Dept. of Electronic and Communication Engineering
HMRITM, Hamidpur
New Delhi, India

***Abstract* – The wireless sensor network (WSN) represent a very promising domain in term of science and technology. They consist of number of autonomous sensor nodes which are deployed in various areas of interest to collect data and cooperatively transmit that data back to a base station. Wireless Sensor Network can be used in a large variety of application due to their easy deployment and their low cost of construction. They are used in Military application, Environmental monitoring application, Health care application etc. Wireless Sensor Network are subject to various form of failures including hardware and different type adversary attacks. However, in hostile scenarios, the network is likely to come under attack from malicious entities which seek to compromise rooting diversity in these environments. Adversaries range from a hacker with laptop to corporation and government's who have a vested interest in compromising the proper operation of an unwelcomed sensor network. Adversaries can launch different type of attack and cryptography is used to counter those attacks. Denial–of–Service (DOS) attack is one of the most common attacks used by different adversaries for creating a fault in any Wireless Sensor Network. The intent of this paper is to present challenges in security of WSN's along with classification of different type of Active (Denial of Service) DOS attack. The problem of security in main type of active DOS attack is also discussed in this paper.**

Keywords – Wireless Sensor Network, Denial-of-Service attack, Active attack, Wormhole attack, Hello Flood attack, Security.

I. INTRODUCTION

Wireless Sensor Networks have become a new research focus in computer and communication fields. Wireless Sensor Network (WSN's) have been suggested to provide a practical and economically viable approach to data gathering with in locations which are difficult or prohibitively expensive to monitor via human activity [1] Sensor Networks consists of hundreds or thousands of self-organising, low –power, low cost wireless nodes deployed masses to monitor and affect the environment. Wireless Sensor Networks were inspired by military applications such as border control but have now become pervasive and are being used in the health industry, in the environment as well as in home applications [2] In these networks, a large number of sensor nodes are deployed to monitor a vast field in hostel unattended environments. For that, they should be equipped with security mechanisms to defend against attacks such as node capture, physical tampering, eavesdropping, denial of service etc. Unfortunately, traditional security mechanisms with high overhead are not suitable for resource constrained sensor nodes due to their lack of processing power, limited memory and energy [3] Wireless Sensor Network usually exist in dangerous or inaccessible areas such as behind enemy lines or other environments with adverse environmental conditions, For example : - Undersea, near active Volcanoes, or out in the wilderness [4] also lack of physical security and vulnerable nature of different sensor for radio communications are characteristics that increase the risk of failure on this type of networks [5].

Adversaries may capture a node and reprogram it and/ or steal sensitive data such as cryptographic keys from it. If these reprogrammed nodes are then inserted back in to the sensor network, they may be used to cause may them such as Jamming, Collisions, Wormhole, Unfairness, Hello Flood, Misdirection, Black Holes and Flooding [6] A variety of attacks are possible in Wireless Sensor Network (WSN). These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks.

Attacks can be classified in to two main categories, according the interruption of communication act, namely Passive Attacks and Active Attacks. From this regard, when it is referred to a passive attack it is said that the attack obtain data exchange in the network without interrupting the communication. When it is referred to an Active attack it can be affirmed that the attack implies the disruption of the normal functionality of the network, meaning information interruption, modification, or fabrication. Denial of Service (DOS) attack is one of the most common active attack in Wireless Sensor Network (WSN). It can be characterized as an attack with the purpose of preventing legitimate users from using a victim computing system or network resource [7] A distributed Denial of Services (DDOS) attack is a large –scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet. Further, DOS attack also have a variety of different adverse attacks. Worm Hole attack and Hello Flood attack are main types of Active DOS attacks.

The rest of this paper is organised as follows:- Section-II gives a brief information about DOS attacks. Section-III describes about Wormhole attack. Section-IV presents detail about Hello Flood attack. Finally, we conclude the paper in Section-V.

II. DENIAL OF SERVICE (DOS) ATTACK

A Denial of Service (DOS) attack or distributed Denial of Service (DDOS) attack is an attempt to make a computer

resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DOS attack may vary, it generally consist of the concerted efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DOS attacks typically target sites or services hosted on high profile web servers such as banks, credit card payment gateways, and even root name servers [8] [9] Denial of Service attack can also lead to problem in network 'Branches' around the actual sensor being attached. For example:- Bandwidth of a router between a Internet and a LAN may be consumed by an attack, compromising not only the intended component, but also entire network or other computer on LAN. Many attack techniques can be used for DoS purpose as long as they can disable service, or downgrade service performance by exhausting resources for providing services. Although it is impossible to enumerate all existing attack techniques. Known DoS attacks in the Internet generally conquer the target by exhausting its resources, that can be anything related to network computing and service performance, such as link bandwidth, TCP connection buffers, application/service buffer, CPU cycles, etc. Individual attackers can also exploit vulnerability, break into target servers, and then bring down services. There are many different DOS attacks, the following illustration shows a major classification of Active DOS attack and we can observe Wormhole and Hello Flood attacks are main type of Active Denial of Service attacks.

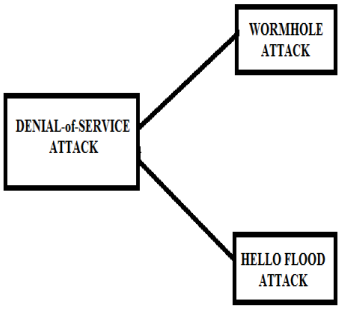

Figure 1. Classification of Active DoS Attack

III. HELLO FLOOD ATTACK

Most sensor network routing protocols are quite simple, and for this reason are sometimes even more susceptible to network attacks as compared to general ad-hoc routing protocols. Most network layer attacks against sensor networks fall into one of the following categories: [10]. Some routing protocol in Wireless Sensor Network requires nodes to broadcast 'HELLO' message to announce themselves to their neighbours. A node which receives such a message may assume that it is within a radio range of the sender. However in some cases this assumption may be false, sometimes a laptop class attacker broadcasting routing or other information with large enough transmission power could convince every other node in the network that the attacker is its neighbour. As a result, the network is left in a state of confusion. If For example :- The attacker advertises a very quick route to a base station in the 'HELLO' packet, many non –neighbour nodes will attempt to route packets through the malicious node. Hence the network is left in a state of confusion. An attacker does not necessarily need to construct legitimate traffic in order to use the Hello flood attack. It can simply re-broadcast overhead packets with enough power to be received by every other node in the network. So, we can say in Hello flood attack many routing protocols use "HELLO" packets to discover a neighbouring nodes and thus to establish the topology of the network. The simplest attack for an attacker consists in sending a flood of such messages to flood the network and to prevent the other messages from being exchanged. The solution for this attack is to verify the bi-directionality of a link before acting on its information.

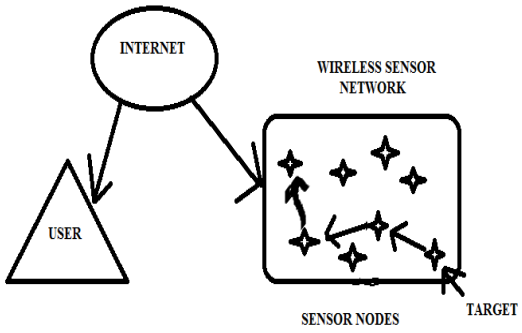

Figure 2. Model of HELLO FLOOD ATTACK

IV. WORMHOLE ATTACK

A devastating attack is known as Wormhole attack, where more than two malicious colluding sensor nodes does a virtual tunnel in the Wireless Sensor Network, which is used to forward message packets between tunnel edge points. Suppose in a wireless sensor network, there is a malicious node 'A'. It will intercept packet from a node and send it to another malicious node 'B' through a special tunnel, and then 'B' replay this packet in the network. In this way, an illusion was created to other nodes in the network that there is a short route between 'A' and 'B'. So, 'A' and 'B' can attract large amount of data flowing through the network to the channel. At this time, malicious nodes 'A' and 'B' can launch security attacks such as selective packet discard in, which will cause damage to normal network functions such as routing, data aggregation and others. In sensor network when sender node sends a message to another receiver node in the network. Then the receiving node tries to send the message to its neighbouring nodes. The neighbour sensor nodes assume that the message was send by sensor node (this is normally out of range) so they tries to forward the message to the originating the node, but this message never come because it is too far away. The main difference between a Wormhole attack and any other

Wireless sensor attack is that there is no need to crack encryption key of the network or capturing legal node, so it has more damage. The problem is that Wormhole nodes may passively relay traffic between end points without participating in routing, so they would not necessarily be visible as network nodes. Wormhole attack is a great threat to sensor network since, this type of attack will not require compromising a Wireless sensor in the network instead; it could be performed even at the starting phase during the sensor initializes to identify its neighbouring information. So we can say Wormhole attack is a active DOS attack, which can be mounted on a wide range of Wireless network protocols without compromising any cryptographic quantity or network node. In the Wormhole model, it is assume that the adversary does not compromise the integrity and authenticity of the communication and any cryptographic quantity remain secret. If any adversary had access to cryptographic keys, it could generate and forge any authentic message, and inject it back into the network with no assistance from Wormhole.

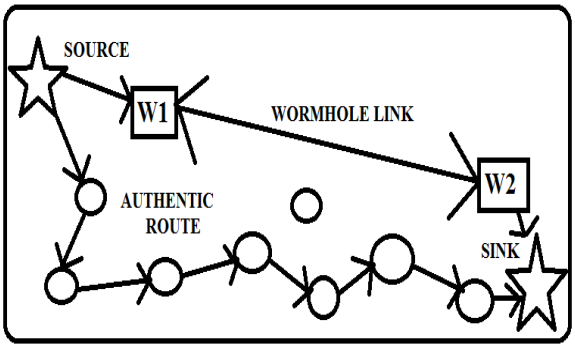

Figure 3. Model of WORMHOLE ATTACK

V. CONCLUSION

Wireless Sensor Network have become promising future to many applications but it's very important to use efficient, reliable and fault tolerance approaches in order to maintain the network connectivity and to increase the data transmission accuracy, especially in presence of faults. As in absence of adequate security, deployments of sensor networks are cause by insertion of false information by compromised nodes within the network. All the discussed security threats, Denial of Service attack, Hello flood attack and Wormhole attack serve one common purpose that is to compromise the integrity of the network they attack.

REFRENCES

[1] K. Romer and F. Mattern, "The design space of wireless sensor networks," Wireless Communications, IEEE, vol. 11, no. 6, pp. 54–61, Dec. 2004.
[2] I. Akyildiz et al., "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, Aug. 2002.
[3] "A survey on wireless sensor network security", J. Sen Int J Commun Netw Inform Secur (IJCNIS), I(2)(2009)
[4] ——, "Security in wireless sensor networks," Commun. ACM, vol. 47, no. 6, pp. 53–57, Jun. 2004. [Online]. Available: http://doi.acm.org/10.1145/990680.99070
[5] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures"; Ad Hoc Networks Vol.1 (2003) pp. 293–315.
[6] A. Wood and J. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002.
[7] David Karig and Ruby Lee, "Remote Denial of Service Attacks and Countermeasures," *Princeton University Department of Electrical Engineering Technical Report CE-L2001-002*, October 2001
[8] Ray Hunt, Network Security: The Principles of Threats, Attacks and Intrusions, part1 and part 2, APRICOT, 2004.
[9] Ehab Al-Shaer, "Network Security Attacks I: DDOS", DePaul University, 2007.
[10] Chris Karlof, David Wagner,(2003) Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, IEEE.