DENIAL OF SERVICE ATTACKS & DETECTION TECHNIQUE IN WSN

Atul Koranga[1], Neeraj Mehra[2], Mayur Srivastava[3]
[1,2]Student Computer Science, Quantum School of Technology, Roorkee, India
[3]Assistant Professor, Quantum School of Technology, Roorkee, India

ABSTRACT

Wireless Sensor Network (WSN) is a deployment of several devices equipped with sensors that perform a collaborative measurement process. Only three processes are involve in wsn sensing data from environment, processing the obtained data, convert it into information and transmit it to the machine for further use. The problem occur when an attacker floods the server or network with large number of continuous packet which the server can't able to process and due to which server or network crashes thus the rightful user and organization are not able to access the resources. This phenomenon is known as DOS attack or Denial Of Service attack.

Keyword used: Denial of Service or DOS, WSN (Wireless Sensor Network),Detection Technique.

I. INTRODUCTION OF DOS ATTACK

DoS attack started as technical competition among underground hackers, attacking any website and taking it down makes the attacker recognition in the underground market. DOS attacks can be performed easily because of the easy to use DOS tools such as XERXES,TRINOO, etc. which are available on the internet, and can easily be used to take down popular websites. Nowadays DOS attacks is being used as a tool to extortion of money, taking out competitors in business and expressing their disagreement with the policies of organization , resources like link bandwidth ,TCP connection buffers, cpu cycles, application /service buffer, etc. which comes under network computing and service performance are the main source of target by an attacker [5].

The attack proceed by flooding the network resources with useless continuous packets. The dos attack makes the network resource unavailable to the rightful user or organization at any given moment of time. In the recent years DOS attacks taken a new form known DDoS (Distributed Denial of Service). The conventional DoS attack aren't very useful as it is difficult to overload server with just one system thus the first step in the DDos attack is taking Control of several systems by using malicious contents or spams thus allowing the attacker to use the compromised system as bots to perform Denial Of Service. The attacker then flood the target network with useless packets with the help of victim bots and making it dicey to identify the main source of attack [2].

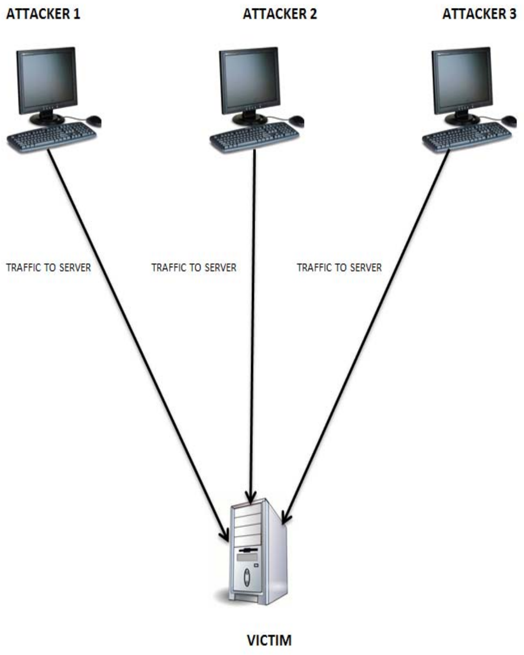

Fig.1 DoS Attack.

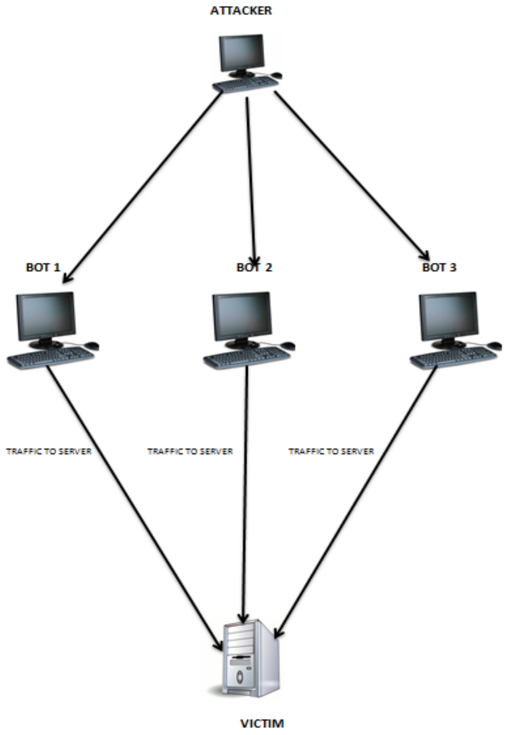

FIG.2 DDoS Attack

II. DOS ATTACKS ON PROTOCOL LAYERS

Layers	Attacks
Application	Overloading Sensors, Path Based Dos, Reprogramming Attack .
Transport	Synchronize flood, Desynchronized Attack.
Network	Spoofing, changing routing control traffic, hello floods and homing.
Data Link	Interrogation, Denial of sleep.
Physical	Jamming and node destruction.

Table 1: Shows attacks on different layers

Our main focus is on the attacks that exploit weaknesses in application and network protocols. We will also mention ways to prevent physical tempering and mitigating sensor over use.

Physical Layer:
Jamming is the easiest way to attack on physical layer jammer can be defined as “we define a jammer to be an entity who is purposefully trying to interfere with the physical transmission and reception of wireless communication”[3]. In laymen language a jammer is used to interrupt the incoming of data packets. There are 4 types of different jammers.

Constant Jammer
A constant jammer continuously produce radio signals on a wireless medium. The produced signals contains random sequence of bits. The main purpose is to fool a legit transmitter into sensing the channel busy thus restrict it from gaining access the channel.

Deceptive Jammer
These jammers are somewhat similar to constant jammers as they continuously transmit bits. The difference is in the transmitted bit as generated bits are not random, deceptive jammers transmit regular packets without any gap in transmission. Thus, fooling a eavesdrop into believing that a legitimate transmission is occurring [4].

Random Jammer
In random jammers an attacker jams the signals for the particular time interval x seconds and then sleeps for time interval y seconds. By changing value of x & y we can change the values of jamming time and power saving time. Thus, making a customized jammer [4].

Reactive Jammer
The Reactive Jammer Attack is a major security threat to wireless sensor networks because reactive jammer attack is a light weight attack which is easy to launch but difficult to detect .This work suggest a new scheme to neutralize malicious reactive jammer nodes by changing the characteristic of trigger nodes to act as only receive [5].

Network Layer:
Sensor network routing vulnerabilities and attack countermeasures were briefly discussed by chris Karlof and David Wagner.[9].Spoofing, replaying or altering routing traffic are the common attacks on routing protocols. These type of attacks can easily be prevented using link layer authentication and anti-replaying.Mainly these are the types of attack in network layer:

Black hole Attack
This Attack is called as Routing layer attack, where the packet transmissions in many number

of nodes from the routing layer. In this attack it is impossible to prevent and mitigate easily. It may prevent temporarily in the networks

Sinkhole Attack

The Attack is the insider Attack, by which the attacker who get inside through the node to the network and fetch the information from the neighbors nodes which is based on the routing protocol. This makes the communication to one or more node that makes the Wireless Sensor Networks vulnerable.

Selective forwarding

It is somewhat similar to black hole attack. In this type of attack the attacker reduce the chances of detection by selectively forwarding random packets. To detect this type of attack we can use implicit acknowledgement which ensures the packets are forwarded instead of being dropped.

Hello flooding

In this type of attack there is no need for compromising encryption. In several routing protocols nodes broadcast hello messages to one hop neighbors to inform their presence [1]. The hello flooding is initiated by recording the hello packets and then transmitting them by high power thus acting as a bridge between the originating node and the next hop which isn't in the range of transmitting node. Thus creating a unreliable packet forwarding route.

Data link Layer:

This layer use MAC protocols and require collaboration between nodes to adjudicate uses of channel. Which make them vulnerable for Dos attack. Two main types of DLL layer attack are Interrogation attack and Denial of sleep attack.

Interrogation Attack

In interrogation attack the two-way request-to-send/clear-to-send (RTC/CTS) handshake is exploited.This handshake is being used by many MAC protocols to alleviate the hidden node problem. The attacker continuously sends RTS messages to exhaust the resources of the neighboring node by making it send CTS response. This can be prevented by using Strom Link Layer authentication and Anti replay protection.

Denial of sleep

In denial of sleep attack, attacker keeps on the radio of wireless sensor network so that it would drain the batteries only in few days.

Transport Layer:

At the transport layer, which manages end-to-end connections, there are mainly two types of Dos attack:

Synchronized Flood Attack

flooding attacks exploit protocols that maintain connection information at either end [11]. Connectionless transport layer protocol has no effect on this type of attack. The SYN cookies is used to prevent this attack, in which client's TCP SYN message's information encode and return it to the client to avoid maintaining state at the server.

Desynchronized Attack

In this attack, an attacker interrupts an active connection between two nodes by transmitting fake packets with fake sequence numbers or control flags that desynchronize endpoints so that they will retransmit data. header authentication is used to prevent this type of attack.

Application Layer:

Mainly Application Layer attacked by following Attacks:-

Overloading Sensors

In this attack an attacker overpower network nodes with sensor stimuli, which makes network to forward large volumes of traffic to a base station, this consumes network bandwidth and drains node energy. This attack reduced by carefully tuning sensors so that only the specifically desired actions activates them. We can also use Rate-limiting and efficient data-aggregation algorithms to reduces this attack [1].

Path Based DoS Attack

In this attack fake and replayed packets injected into the network at leaf node [7]. The packet is forwarded to its destination, nodes along the path to the base station waste bandwidth and energy transmitting the traffic. This attack can starve the network of lawful traffic, because it consumes resources on the path to the base station, thus preventing other nodes from sending data to the base station . We can prevent these attacks by Combining packet authentication.

III. DETECTION OF DoS ATTACKS ON WSN

Lightweight detection using BLINC

It is a lightweight method proposed by Sirikarn Pukkawanna, Vasaka Visoottiviseth, Panita Pongpaibool[12] which analyses the host behavior to detect DoS attacks. this method uses the concept of BLINd classification /BLINC i.e. without accessing the payload in packet, without knowing the port numbers etc. the only known thing is about what current flow collectors provide. BLINC maps flows of packets into graph lets for each attack pattern. Unlike conventional IDS which uses pre-defined signatures and behavior patterns to detect attacks this method takes a different approach by comparing the graph lets of different attacks patterns with incoming traffic records or logs. This method shows a high true positive rate and a very low false positive rate.

Detection using Kolmogorov Complexity Metrics

This method is briefly explained by A.B. Kulkarni, S.F. Bush, and S.C. Evans[10] to detect the detecting distributed denial of service (DDoS) attacks. This technique is based on the concept of Kolmogorov complexity. Kolmogorov complexity states that the sum of the complexities of the individual strings is greater than the joint complexity measure of random strings, if the strings show some correlation. The given algorithm uses this method to find a relation between traffic flows in the network and identify DoS attacks. The main benefit of using Kolmogorov algorithm is that it no special filtering is required and thus it can detect any type of distributed denial of service attack. The performance of this method is far ahead than that of load measuring or packet counting methods.

Detection using improvised Honeypots

This method is explained in detail by Vinu V Das[14]in his research. Honeypots are the virtual or physical systems used for detecting infected hosts by acting as intrusion detection tool. A honeypot simply acts as a detection server from the pool of severs in a network. This method is an improvement to the existing honeypot method which has some vulnerabilities like legitimate attacker and Link Unreachable problem. The legitimate attacker problem is solved by creating a virtual/physical communication port for a authorized user and for rest of the nodes active server acts as virtual or physical honeypot. The Link unreachable problem is mitigated by opening a temporary communication route through honeypot for the authorized user or client by acting as a active server virtually and for the rest of the unauthorized nodes, ASs and for attacker it still acts as honeypot and prevent intrusion and attacks. This method is quite efficient in addressing the conventional challenges and is quite secure.

Clustering technique

Dos attacks targets the energy consumption in order to degrade the overall Quality of Service (QoS). In this technique energy-preserving solution is used to detect compromised nodes in WSNs by elect Controlled nodes that analyze the traffic inside a cluster and to send warnings to the cluster-head whenever an abnormal behavior is detected. This technique is dynamic as the Controlled nodes are periodically elected among ordinary nodes on each cluster. Such planning results in a better energy balance while maintaining good detection coverage as it is based on the distance between nodes, the output throughput and delay between packets transmission [13].

IV CONCLUSION

In this paper we have mentioned different types of DoS attacks and their mitigation on wireless sensor network among different layers of the OSI model. These attacks degrade the Quality of Services of network by exhausting their resources and prevent the legitimate user from accessing these resources. We have also discussed different detection techniques like clustering technique, using improvised honey pots, Kolmogorov algorithm and using graph lets to detect Denial of Service attacks on protocol layers. There is still many scope is remain in this field, so one can work on different energy efficient detection technique on DoS attack in WSN.

REFERENCES

[1] Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks:

Attacks and defenses. IEEE Pervasive Computing, 7(1).

[2] Yu, J., Li, Z., Chen, H., & Chen, X. (2007, June). A detection and offense mechanism to defend against application layer DDoS attacks. In Networking and Services, 2007. ICNS. Third International Conference on (pp. 54-54). IEEE.

[3] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” MobiHoc 05, May 25-27, 2005, Urbana-Champaign, Illinois, USA, pp 46-57.

[4] Pelechrinis, K., Iliofotou, M., & Krishnamurthy, S. V. (2011). Denial of service attacks in wireless networks: The case of jammers. IEEE Communications Surveys & Tutorials, 13(2), 245-257.

[5] Gu, Q., & Liu, P. (2007). Denial of service attacks. Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications, 3, 454-468.

[6] Shivanagu, R., & Deepti, C. A Security Mechanism Against Reactive Jammer Attack In Wireless Sensor Networks Using Trigger Identification Service.

[7] J. Deng, R. Han, and S. Mishra, “Defending against Path-Based DoS Attacks in Wireless Sensor Networks,” Proc. 3rd ACM Workshop Security of Ad Hoc and Sensor Networks, ACM Press, 2005, pp. 89–96.

[8] 9. D. Raymond et al., “Effects of Denial of Sleep Attacks on Wireless Sensor Network MAC Protocols,” Proc. 7th Ann. IEEE Systems, Man, and Cybernetics (SMC) Information Assurance Workshop (IAW), IEEE Press, 2006, pp. 297–304.

[9] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Proc. 1st IEEE Int’l Workshop Sensor Network Protocols and Applications, IEEE Press, 2003, pp. 113–127.

[10] Kulkarni, A., & Bush, S. (2006). Detecting distributed denial-of-service attacks using kolmogorov complexity metrics. Journal of Network and Systems Management, 14(1), 69-80.

[11] . A.D. Wood and J.A. Stankovic, “Denial of Service in Sensor Networks,” Computer, vol. 35, no. 10, 2002, pp. 54–62.

[12] Pukkawanna, S., Visoottiviseth, V., & Pongpaibool, P. (2007, November). Lightweight detection of DoS attacks. In Networks, 2007. ICON 2007. 15th IEEE International Conference on (pp. 77-82). IEEE.

[13] Mansouri, D., Mokdad, L., Ben-Othman, J., & Ioualalen, M. (2013, April). Detecting DoS attacks in WSN based on clustering technique. In Wireless Communications and Networking Conference (WCNC), 2013 IEEE (pp. 2214-2219). IEEE.

[14] Das, V. V. (2009, January). Honeypot scheme for distributed denial-of-service. In Advanced Computer Control, 2009. ICACC'09. International Conference on (pp. 497-501). IEEE.