DENIAL OF SERVICE ATTACKS AND COUNTER MEASURES IN WIRELESS SENSOR NETWORK

Ankur Rana[1], Jaspreet Srivastava[2], Mayur Srivastava[3]
[1,2]Asstt. Prof, CSE, Quantum School of Technology, Roorkee-India
[3]Research Scholar, Uttrakhand Technical University, Dehradun

Abstract
Denial of Service (Dos) attacks can be easily launched in Wireless Sensor Networks due to its unattended nature. In denial-of-service attack (DoS attack) attacker make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. This paper addresses different DoS attacks and there countermeasures on different layers in WSN.
Keywords: Wireless Sensor Networks (WSN), Denial of Service (Dos), Security.

I INTRODUCTION

Denial of service attack has a major threat to the current computer network. DoS attacks are, in essence, resource overloading attacks and are capable of either, crashing the host such that it cannot communicate properly with the rest of the network [1, 2]. The attack overloads the servers or networks with useless traffic such that the server spends so much time handling the attack traffic such that it cannot attend to its real work [9].In WSN, ensuring security is very challenging task because of various limitations like – memory, battery power and computational capabilities. As sensors are deployed in a unattended manner in a WSN environment hence an adversary can easily launch a various types of attacks [18].In this paper we present different types of attacks and there countermeasures. In section 2 we describe the related work of WSN security. In section 3 we define different types of DoS attacks. And we conclude our study in section 4.

II RELATED WORK

[9] Explores the architecture of internet and here focus is only on functionality and not the security. The casual users leave their computer vulnerable to compromise. For example, using the password which is given by the vendors at the time of purchase, leaving auto configure features in default setting. The CERT Program is part of the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. The CERT coordinate center, the center of Internet security expertise, has identified 831 key vulnerabilities in the Internet architecture and suggests that automated tools are being used to exploit these security holes.“brute-force” jamming techniques, which mainly exploit PHY and MAC layer vulnerabilities, can be detected easily. Jammers have responded by employing more intelligent ways to accomplish jamming task in order to evade detection. They exploit vulnerabilities at the higher layers of the network stack [3]. A typical example is detecting the transmission of specific control packets and preferentially corrupting such packets by injecting interference. In order to address these threats, security experts must deploy more efficient methods for detecting and preventing such “smart” (stealthy) attackers. A fascinating arms-race, thus, begins between adversaries and network administrators [16].

III DIFFRENT DOS ATTACKS AND COUNTER MEASURES

In this section we describe the different DoS attacks on different level and there countermeasures.

Wormhole Attack: Wormhole attack is a significant threat to wireless sensor networks, because, this sort of attack does not require compromising a sensor in the network rather, it

could be performed even at the initial phase when the sensors start to discover neighboring information. Wormhole attacks are difficult to counter because routing information supplied by a node is difficult to verify.

Prevention of Wormhole attack: The prevention mechanism for wormhole attack include, DAWWSEN [11] , a proactive routing protocol based on the construction of a hierarchical tree where the base station is the root node, and the sensor nodes are the internal or the leaf nodes of the tree. A great advantage of DAWWSEN is that it doesn't require any geographical information about the sensor nodes, and doesn't take the time stamp of the packet as an approach for detecting a wormhole attack, which is very important for the resource constrained nature of the sensor nodes.

Black hole Attack: A Black hole is a malicious node that falsely replies for any Route Request (RREQ) without having active route to specified sink and drops all the receiving packets. If such compromised nodes work together in a group, then damage caused will increase significantly. Such attack is sometime referred as cooperative Black-Hole attack [20].

Prevention of Black hole attack: REWARD (receive, watch, redirect) algorithm. This algorithm utilizes two types of broadcast messages, MISS and SAMBA.

Layer	Attacks	Defense
Physical	Jamming	Priority message, region mapping, mode change
Link	Crash Exhaustion Unfairness	Error correcting code Rate limitation Small Frames
Network	Spoofed & Selective forwarding Sinkhole Sybil Wormhole Grayhole& Blackhole Hello Flood	Authentication, Monitoring, Filtering Redundancy Probing Authentication, Monitoring, redundancy Authentication, Probing Monitoring, authentication Authentication, Packet curbs by using geographic & temporal info.
Transport	Flooding De-synchronization	Client puzzles Authentication

Table 1: shows attacks on different layers and its defenses

MISS (Material for intersection of suspicious sets) message. SAMBA (Suspicious area mark a Black hole attack) message.

Sybil Attack: In a Sybil attack an attacker try to make fool several identification in a particular region. As same frequency is shared among all the nodes and only single communication is broadcasted so for this reason a chance of Sybil attack is increases rapidly in wireless sensor network [12].

- Prevention of Sybil attack: The mechanisms to prevent against Sybil attacks are to utilize identity certificates [13]. The basic idea is very simple. The setup server, before deployment, assigns each sensor node some unique information. The server then creates an identity certificate binding this nodes identity to the assigned unique information, and downloads this information into the node. To securely demonstrate its identity, a node first presents its identity certificate, and then proves that it possesses or matches the associated unique information.
- Selective Forwarding attack: It is a situation when certain nodes do not forward many of the messages they receive. The sensor networks depend on repeated forwarding by broadcast for messages to propagate throughout the network.
- Prevention of selective forwarding attack: Multipath routing can be used to counter these types of selective forwarding attacks. Messages routed over paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most compromised Allowing nodes to dynamically choose a packets next hop probabilistically from a set of possible candidates can further reduce the chances of an adversary gaining complete control of a data flow [14].
- Sink Hole Attack: The aim of sinkhole attack is to misguide all the traffic from a particular area of the network through a compromised node, creating a metaphorical sinkhole with the adversary at the center [15].
- Prevention of sink hole attack: Such attacks are very difficult to defend against. One class of protocols resistant to these attacks is geographic routing protocols. Geographic protocols construct a topology on demand using only localized interactions and information and without initiation from the base station [16].

IV CONCLUSION

All the previous attacks show one thing common that is to compromise the integrity of the network they attack. In this paper we mainly focus on the security threats and we conclude that the defense mechanism present over here just provide the blueprint about the WSN security threat.

There are many security tools are used on layer-by-layer basis. With this paper we provide many common attacks on different layer of OSI model and their best possible solution.

REFERENCES

[1]. Deng, J., Han, R., & Mishra, S. (2005, November). Defending against path-based DoS attacks in wireless sensor networks. In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (pp. 89-96). ACM.

[2] Rothery, M. (2005). Critical infrastructure protection and the role of emergency services. Australian Journal of Emergency Management, the, 20(2), 45.

[3] Pathan, A. S. K., Lee, H. W., & Hong, C. S. (2006, February). Security in wireless sensor networks: issues and challenges. In Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference (Vol. 2, pp. 6-pp). IEEE.

[4] Liu, Z., & Uppala, R. (2006, September). A dynamic countermeasure method for large-scale network attacks. In Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on (pp. 163-170). IEEE.

[5] Cao, Z., Zhou, X., Xu, M., Chen, Z., Hu, J., & Tang, L. (2006, September). Enhancing base station security against DoS attacks in wireless sensor networks. In Wireless Communications, Networking and Mobile Computing, 2006. WiCOM 2006. International Conference on (pp. 1-4). IEEE.

[6] Deng, J., Han, R., & Mishra, S. (2006). Limiting DoS attacks during multihop data delivery in wireless sensor networks. International Journal of Security and Networks, 1(3-4), 167-178.

[7] Walters, J. P., Liang, Z., Shi, W., & Chaudhary, V. (2006). Security in distributed, grid, and pervasive computing. Wireless sensor network security: A survey.

[8] 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.

[9] Karthik, S., Bhavadharini, R. M., & Arunachalam, V. P. (2008, December). Analyzing interaction between denial of service (dos) attacks and threats. In Computing, Communication and Networking, 2008. ICCCn 2008. International Conference on (pp. 1-9). IEEE.

[10] Cao, X., Kou, W., Dang, L., & Zhao, B. (2008). IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks. Computer communications, 31(4), 659-667.

[11] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, (2005)" DAWWSEN: A Defense Mechanism against Wormhole attack In Wireless Sensor Network", Proceedings of the Second International Conference on Innovations in Information Technology (IIT'05).

[12] Demirbas, M., & Song, Y. (2006, June). An RSSI-based scheme for sybil attack detection in wireless sensor networks. In Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks (pp. 564-570). IEEE Computer Society.

[13] J. R. Douceur, (2002) "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS '02).

[14] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks,"Mobil Computing and Communications Review, vol. 4, no. 5, October 2001..

[15] Hamedheidari, S., & Rafeh, R. (2013). A novel agent-based approach to detect sinkhole attacks in wireless sensor networks. Computers & Security, 37, 1-14.

[16] M. Zorzi and R. R. Rao, (2003) "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance," IEEE Transactions on Mobile Computing, vol. 2, no. 4, pp. 337-348, 2003

[17] Manju, V. C., & Kumar, M. S. (2012, December). Detection of jamming style DoS attack in Wireless Sensor Network. In Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on (pp. 563-567). IEEE.

[18] Bahl, N., Sharma, A. K., & Verma, H. K. (2012). On Denial of Service Attacks for Wireless Sensor Networks. SYSTEM, 17, 18.

[19] Ramesh, M. V., Raj, A. B., & Hemalatha, T. (2012, November). Wireless Sensor Network Security: Real-Time Detection and Prevention of Attacks. In Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on (pp. 783-787). IEEE

[20] Srivastava, M., & Dixit, A. BLACKHOLE DETECTION TECHNIQUE IN WSN-A REVIEW.