Volume 6, Issue 6, June 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review of Prevention Techniques for Denial of Service Attack in Wireless Sensor Network

Poonam Rolla, Manpreet Kaur, Jabarweer Singh
Department of CSE, GZS Campus College of Engineering and Technology, Bathinda, Punjab, India

Abstract— Wireless Sensor Network (WSN) is an auspicious technology that has tremendous potential for various futuristic applications. As WSN become wide spread, security becomes a cardinal affair. One of the terrible threats is Distributed Denial of Service (DDoS) that not only affects the network bandwidth but also affects the performance of the network. Various mechanisms are there in the literature that provides solution to avert DDoS attack. A review on DDoS detection and prevention techniques have been done in this paper.

Keywords---- DOS Attacks, Prevention techniques, Security Goal, Wireless sensor network.

I. INTRODUCTION

Basically, Sensor networks are mainly designed for real time data processing in complicated environment. A WSN is a wireless network consists of large number of tiny sensor nodes used to monitor environmental conditions like temperature, sound etc. There are many applications of wireless sensor networks like military and traffic surveillance, natural disaster detection and many more. These applications often feature the monitoring of sensitive information such as opposition movement on the battleground; therefore Security is primary issue in WSNs.

In WSN, DDOS (Distributed Denial of service) attack makes powerlessness network. The packets travel several times in the sensor network .By that all the resources like bandwidth, memory, energy are worthless by this attack. By controlling these kinds of attacks network performance can be improved. The main aim of this paper is to review effect of various attacks in wireless sensor network and their prevention techniques.

This paper includes introduction of Wireless Sensor Networks and DDoS attack in Section 1, prevention techniques proposed for DOS attacks are reviewed in section 2, section 3 defines comparative analysis of different techniques and Section 4 concludes the paper.

II. RELATED WORK

In this paper [2] authors proposed a scheme using game theoretic approach to prevent DoS attacks in WSN. This technique uses two concepts: One is utility based source routing that computes the total utility of each source route in data packets. This routing scheme is a dynamic routing scheme. The other theory is based on a reputation list where each node earns rating from its neighboring nodes. The disadvantages in this scheme are the node that has less reputation does not get selected in source routing and difficult to detect compromised nodes if the nodes are large in number.

In this paper [3] an ant-based framework that exploits the significance of stateless and state full signatures therefore preserving the legitimate packets only, in this manner discarding the contaminated packets has been proposed. The disadvantage of this scheme is, it only detects flooding attack.

The scheme proposed in paper [4] is a flexible novel framework against DoS attacks. This is a hierarchal framework having two important stages: attacks detection stage and defending stage where various defensive methods are proposed to overcome detected attacks. By this scheme flooding, exhaustion, and jamming attacks can be detected.

A novel cluster based intrusion detection technique is proposed in [5] to prevent DoS attacks essentially misdirection attacks. This technique builds the clusters from mobile nodes that are in their communication range with each other. Among these nodes a node is nominated as cluster head (CH) based on two things that are fairness probability of a node as a CH should be equivalent and efficiency- a node having high efficiency should be selected periodically from the cluster.

In this paper [6] has proposed a profile based protection scheme (PPS security scheme against DDoS attack. Main aim of this paper is visualize the effect of DDoS attack in network and identify the nodes that are affected the performance of the network. The profile based scheme check the profile of each node and only the attacker is the node that flooded the unnecessary packets then PPS has block the performance of attacker.

In this paper [7] has proposed routing protocol that is implemented and simulated in NS2 environment. In order to simulate the performance with the help of two different network scenarios the performance is compared and the comparative performance study is performed in the form of packet delivery ratio, throughput, energy consumption and end to end delay. The results demonstrate the performance with respect to the traditional routing protocol.

III. COMPARATIVE ANALYSIS OF TECHNIQUES

TABLE I. COMPARATIVE ANALYSIS OF TECHNIQUES

Proposed method in	Advantages	Disadvantages
(2) May 2007	Dynamic routing mechanism	The node that has less reputation doesn't get selected in source routing and difficult to detect compromised nodes if the nodes are large in Number.
(3) June 2010	It helps in tracing the source of attack without applying any specific trace back technique	Only flooding attacks can be detected.
(4) 2011	Can maps the jamming, flooding and exhaustion affected areas Exactly.	Only jamming, flooding, and exhaustion attacks can be detected.
(5) 2013	It can maps the misdirection attacks affected Area.	Detects only misdirection Attacks.
(6) 2014	Provides 100% performance.	Takes too much time to check the profile of each node.
(7) Feb 2015	Preventing the malicious nodes in network by consuming the historical data for estimating the Decisional threshold.	Only vampire attack can be detected and prevented.

IV. CONCLUSION

Wireless sensor network is the network having number of nodes; these nodes forward the packets from one node to another continuously. So in that moment network is affected from the Distributed Denial of Service attacks. DDoS attack loss the major resources like energy, bandwidth, and power etc .In this paper we review several techniques to protecting DDoS attack. Inventive approaches to DDoS defense will be designed. They will also offer new design features carrying their share of remuneration and weaknesses. We expect these techniques to offer a foundation for classifying threats and defenses in DDoS field. As the field grows, the techniques will also grow and be refined.

REFERENCES

[1] Chan, Haowen, and Adrian Perrig. "Security and privacy in sensor networks." *Computer* 36.10 (2003): 103-105.

[2] Agah, Afrand, Mehran Asadi, and Sajal K. Das. "Prevention of DoS Attack in Sensor Networks using Repeated Game Theory." *ICWN*. 2006.

[3] Juneja, Dimple, and Neha Arora. "An ant based framework for preventing DDoS Attack in wireless sensor networks." *arXiv preprint arXiv:1007.0413* (2010).

[4] Yang, Xin, et al. "A novel framework of defense system against DoS attacks in wireless sensor networks." *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on*. IEEE, 2011.

[5] Sachan, Roshan Singh, et al. "A cluster based intrusion detection and prevention technique for misdirection attack inside WSN." *Communications and Signal Processing (ICCSP), 2013 International Conference on*. IEEE, 2013.

[6] Nigam, Vivek, Sonal Jain, and Kavita Burse. "Profile based scheme against DDoS attack in WSN." *Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on*. IEEE, 2014.

[7] Dubey, Megha, Mayank Bhatt, and Rajat Bhandari. "Prevention of DDOS Attack in Wireless sensor network using secure routing." *Prevention* 4.2 (2015).

[8] M. Kaur, A. Jain and A. K. Goel, "Energy Efficient Two Level Distributed Clustering Scheme to Prolong Stability Period of Wireless Sensor Network", *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 68-73

