Analysis of Various DDOS attacks Isolation Techniques

[1]Surbhi Jain, [2]Aishwarya Kulshrestha
[1]Research Scholar, Rajasthan College of Engineering for Women, Jaipur
[2]Assistant Professor, Rajasthan College of Engineering for Women, Jaipur
([1]surbhics2011@gmail.com,[2]ashwaryk@gmail.com)

Abstract-The wireless sensor network is the decentralized type of network in sensor nodes can join or leave the network when they want. Due to such type of network malicious nodes enter the network which triggers various types of active and passive attacks. The DDOS attack in the active type of attack which affects network performance. In this paper, various security techniques are reviewed and analyzed in terms of certain parameters

Keywords-*WSN; Active attack; DDOS.*

I. INTRODUCTION

Wireless sensor networks (WSN) consists sensor nodes and base station. There are large numbers of small, low power, low cost sensor nodes with limited memory, computational, and communication resources, to monitor the physical aspects. WSN also consists of spatially distributed autonomous sensors and a Base Station to co-operatively pass their data through the network to a main node or central location. The environmental conditions are continuously monitored by the nodes of WSN to collect detailed information about the physical environment in which they are installed. Further the collected data is transmitted to base station (BS). The BS act as gateway between the sensor networks and the outside world. The BS also has very large storage and large data processing capabilities [1]. The main work of BS is to pass the data it receives from the sensor nodes to the server from where end user can access them. The sensors nodes are generally expand around the area of the Base Station and further as per the need of BS groups were formed. The Sensor nodes have short lifetime because it runs on batteries and once nodes are deployed their batteries cannot be recharged. Modern wireless sensor networks are bi-directional, allowing transmission of information being monitored from nodes to central node or base station, as well as enabling control of sensor activity from base station to sensors [2]. The main advantage of WSN is that it can operate unattended in the environment, where the continuous human monitoring can be risky, inefficient or infeasible. The unique characteristics of WSNs is that it have unique characteristics such as low duty cycle, power constraints and limited battery life, redundant data acquisition, heterogeneity of sensor nodes, mobility of nodes, and dynamic network topology, etc. The development of wireless sensor networks was motivated primarily by military applications such as battlefield surveillance but now WSN is use in various other applications such as in military and health applications [3]. Also they are applied in robot control, automatic manufacturing, office or home automation. WSN is also useful in detecting forest fires based on temperature information it receives from large number of distributed sensor nodes. There are number of attacks possible in WSN. In Wormhole type of attack, malicious nodes make a tunnel which is hidden from the other genuine nodes. The data packets are sent from one malicious node to another via that tunnel, that is, the malicious node attract the packets from one area and passes them to other malicious node in another area. Tunnel can be made through many ways such as in-band and out-of-band. To launch this attack, there is no need to compromise the other genuine network nodes. Therefore, this operation can extremely affect the routing procedures and the localization and can also launch attacks such as eavesdropping, replay attacks etc. against traffic packets. This attack can be established by using following techniques: wormhole using encapsulation, packet relay, high power transmission, out-of-band channel [4]. An attacker does the re-programming in the captured set of nodes in the network in order to block the packets to cause Black hole attack in the network. Once the intruder has been able to intrude himself into the communication network he can do anything with the captured packets passing between them and can generate false messages in spite of forwarding them to the base station in WSN. A malicious node forges the identities of many other nodes which cause Sybil attack. This malicious node can strongly influence the systems in which there is no centralized entity which can verify the identity of each communicating node. So this attack can occur in multipath routing, distributed systems etc. [5]. HELLO flood attack uses HELLO packets in order to convince and attack other nodes in the network. The HELLO packets help the nodes to announce themselves to the neighboring nodes [6]. A node which receives these HELLO packets assumes that it is within the radio range of the sender. But sometimes this assumption prove out to be wrong when the malicious sender sends HELLO packets at such a high speed and processing power to a number of sensor nodes deployed over a wide area within a WSN such that it might convince every other node in the network that the attacker is their neighbor. Consequently, when nodes send the information to the base station they send via the malicious node because they think that the malicious node is in their neighbor. The aim of Denial of Service (DOS) attack is to make network resources unavailable temporarily. In WSN various types of DDOS attacks at various layers can be performed [7]. For example, at physical layer it is tempering and jamming, at data link layer it is exhaustion and collision, at network layer it is homing, misdirection and black hole, at transport layer it can be performed by de-synchronization and flooding. Physical attacks Unlike the previous attacks, physical attacks are irreparable. Attackers can change the programming of the sensors or can replace a particular sensor with an illegitimate sensor which is under their control, can modify the associated circuitry etc.

Distributed Denial of Service (DOS) attack:

The purpose of this attack is to prevent authentic users from using website, web service or computer system like specified network resource. It is a coordinated attack of given target network or system availability. This attack is indirectly launched through many compromised computing systems [8]. The secondary victims are those that are used to launch the compromised systems and primary victims are those that attack the services. The use of secondary victims in a DDoS attack provides the attacker with the ability to wage a much larger and more disruptive attack while remaining anonymous since the secondary victims actually perform the attack making it more difficult for network forensics to track down the real attacker. In Distributed Denial of service attack, the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network is called jamming. Jamming may come in two forms. Constant jamming: This type of jamming implies the jamming of the entire network. In Intermittent jamming, messages are periodically exchanges by sensor nodes [9]. The communication protocols can be intentionally violated by attacker in link layer, e.g., ZigBee or IEEE 802.11b protocol and in order to attempt collisions messages are continuously transmitted. The packets lost by collision are needed to retransmit. By refusing routing messages a multi-hop network advantage is taken by node in routing layer. The conclusion is that any node that is affected by attacker will not be able to exchange messages with the part of network [10]. In case of flooding, that transport layer is also affected by attack. Number of connection requests is send to malicious node in case of flooding. The connection requests are handled by allocating resources.

In this type of attack an attacker sends millions of packets or useless traffic simultaneously to a server and attempting to slow the server or making the resources unavailable to the users and hence due to which a user cannot able to access the facility. The Fig. 1 shows the diagram of Distributed Denial of Service attack. It consists of six nodes or computers name as A, B, C, D and E. In this an attacker i.e. computer A will send request or packets to compromised computers say computer B, C, D, E, F and then these compromised computers simultaneously flood the server (computer G) with thousand and millions of requests. And hence user can't access the resources.

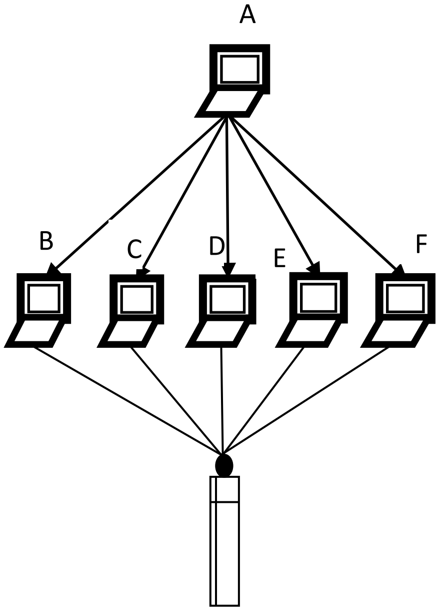

Fig. 1: DDoS attack in WSN

II. LITERATURE REVIEW

Taranpreet Kaur, et.al, (2016), have analyzed that Wireless Sensor Networks (WSNs) is a collection of large number of sensor nodes that have limited capabilities for collecting sensitive information. There is advancement in this technology that leads to security as major concerns. In WSN, there are number of attacks like Distributed Denial of Service (DDOS) attacks. In case of this attack, many attacks are adapted by malicious node such as flooding attack, black hole attack and warm hole attack in order to disturb the overall functionality of network. When it is used in military and industrial applications the risks are more. In order to detect and prevent DDOS attacks, number of researchers has proposed new mechanisms. In this paper [11], authors did a survey on different existing approaches on basis of various parameters. This survey will help researchers to improve the existing techniques that have low false alarm problem and less energy consumption.

Shital Patila, et.al, (2016), have analyzed that Wireless Sensor Networks (WSN) has wide applications in data gathering and data transmission. The most popular attack that effect sensor node is Denial-of-Service (DoS) attack. So, there is need to prevent Dos attack using different techniques. There are number of techniques that have been used by different researchers for preventing DDoS attack. In this paper [12], authors have proposed an improved Co-FAIS immune system for DoS attack in WSN. Co-FAIS immune system is the first real time intrusion detection model that compares current system with normal system to recognize the attack by using fuzzy logic. Authors have improved the current Co-FAIS system by adding two learning parameters in fuzzy system that helps in improving the accuracy rate of detection and improves learning capabilities. The simulation results show that the proposed system will improve the accuracy rate of attack prevention, reduce the false alarm rate that helps in recognizing different DoS attack.

Raksha Upadhyaya, et.al, (2016), have analyzed that open nature of wireless sensor networks (WSN) results in more vulnerability to outside attacks. In this paper [13], authors have proposed a solution to prevent WSN from DDOS attack. In proposed solution they have used dynamic source routing (DSR). The concerned nodes energy is used for detecting and preventing attacks. The proposed scheme provides a modified DSR with security aware mechanism for DDOS attack. The whole process is carried out in four steps. The DDOS attack is prevented by examine battery charge of each node that provides identification of malicious node. A shutdown method has been used to ignore malicious node in the network as DSR doesn't have any blacklist for sensor network. This will help in removing the malicious node from communication and start transferring packet transmission from alternative routes. The proposed scheme is implemented using Qualnet 5.2 simulator.

Raksha Upadhyay, et.al, (2015), have recommended that wireless network with sensing and processing information merit is known as wireless sensor network (WSN). WSN consists of small sensor nodes with transducer, battery, microprocessor along with storage media. The aim of Distributed Denial of Service (DDOS) attack is to disrupt the network by draining resource capability. The attacker will sends worthless messages to increase the network traffic and also degrades the life of node and network. The life of network is directly proportional to battery capacity that draining in battery energy directly degrades the life of node. In this paper [14], severe problems have been observed by authors and a solution is proposed a solution to overcome the problem of power draining due to DDOS attack. In order to simulate and evaluating the performance of proposed solution for AODV and DSR routing protocols in WSN they have used Qualnet 5.0 simulator.

Varsha Nigam, et.al, (2014), proposed a profile based protection scheme (PPS security scheme against DDoS (Distributed Denial of Service) attack [15]. The main reason of this attack is flooding access amount of unnecessary packets in network by that the network bandwidth are consumed by that data delivery in network are affected. The main aim of authors is to visualize the effect of DDoS attack in network and identify the nodes that affect the performance of network. The profile of each node in network is checked by profile based security scheme and only the attacker is one of the node that flooded the unnecessary packets in network then PPS has block the performance of attacker. The performance of network is measured on the basis of performance metrics like routing load, throughput etc. The simulation results are represents the same performance in case of normal routing and in case of PPS scheme, it means that the PPS scheme is effective and showing 0% infection in presence of attacker.

Table. 1: Table of Comparison

Authors' Names	Year	Description	Outcomes
Taranpreet Kaur, Dr. Krishan Kumar Saluja, Dr Anuj Kumar Sharma	2016	In this paper [18], authors did a survey on different existing approaches on basis of various parameters.	This survey will help researchers to improve the existing techniques that have low false alarm problem and less energy consumption.
Shital Patila, Sangita Chaudhari	2016	Authors have proposed an improved Co-FAIS immune system for DoS attack in WSN. Co-FAIS immune system is the first real time intrusion detection model that compares current system with normal system to recognize the attack by using fuzzy logic.	The simulation results show that the proposed system will improve the accuracy rate of attack prevention, reduce the false alarm rate that helps in recognizing different DoS attack.
Raksha Upadhyaya, Uma Rathore Bhatta, Harendra Tripathia	2016	Authors have proposed a solution to prevent WSN from DDOS attack. In proposed solution they have used dynamic source routing (DSR).	A shutdown method has been used to ignore malicious node in the network as DSR doesn't have any blacklist for sensor network. This will help in removing the malicious node from communication and start transferring packet transmission from alternative routes.
Raksha Upadhyay, Salman Khan, Harendra Tripathi, Uma Rathore Bhatt	2015	Severe problems have been observed by authors and a solution is proposed a solution to overcome the problem of power draining due to DDOS attack.	In order to simulate and evaluating the performance of proposed solution for AODV and DSR routing protocols in WSN they have used Qualnet 5.0 simulator.
Varsha Nigam, Saurabh Jain, Dr. Kavita Burse	2014	A profile based protection scheme (PPS security scheme against DDoS (Distributed Denial of Service) attack was proposed in this paper.	The simulation results are represents the same performance in case of normal routing and in case of PPS scheme, it means that the PPS scheme is effective and showing 0% infection in presence of attacker.

III. CONCLUSION

In this paper, it is concluded that wireless sensor network is the decentralized type of network in which malicious nodes trigger various type of attacks. The DDOS attack is the active type of attack which affects network performance. In this paper, various techniques for the isolation of DDOS attack reviewed and discussed. In future, novel approach will be designed for the isolation of DDOS.

REFERENCES

[1] Sukhwinder Sharma, Rakesh Kumar Bansal, Savina Bansal, "Issues and Challenges in Wireless Sensor Networks", IEEE International Conference on Machine Intelligence Research and Advancement, vol 4, pp.58-62, 2013.

[2] M.H. Anisi, A.H. Abdullah, S.A. Razak, "Energy-Efficient Data Collection in Wireless Sensor Networks", Wireless Sensor Networks, vol. 3, pp. 329-333, 2011.

[3] Gouvy, N., Hamouda, E., Mitton, N., & Zorbas, D., "Energy efficient multi-flow routing in mobile Sensor Networks", IEEE In Wireless Communications and Networking Conference (WCNC), vol. 3, pp. 1968-1973, 2013.

[4] Kaur, K., & Kumari, N. Evaluation and Analysis of Active RFID Protocol in Wireless Sensor Networks, vol. 3, pp. 121-129, 2010.

[5] Jiang, L., Bing Fang, & Li., "Energy optimized approach based on clustering routing protocol for wireless sensor networks", CCD Conference. IEEE, vol. 5, pp. 181-190, 2011.

[6] Wang, Y., & Guo, S., "Optimized energy-latency cooperative transmission in duty-cycled wireless sensor networks", In Mechatronics and Automation (ICMA), 2013 IEEE International Conference on, vol. 5, pp. 185-190, 2013.

[7] Neamatollahi, P., Taheri, H., Naghibzadeh, M., & Yaghmaee, M., "A hybrid clustering approach for prolonging lifetime in wireless sensor networks", IEEE In Computer Networks and Distributed Systems (CNDS), 2011 International Symposium on, vol. 6, pp. 170-174, 2011.

[8] Gowrishankar.S, T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar, "Issues in wireless sensor networks", WCE, vol.1, pp 5-15, 2008.

[9] M.H. Anisi, A.H. Abdullah, S.A. Razak, "Energy-Efficient Data Collection in Wireless Sensor Networks", Wireless Sensor Networks, vol. 3, pp. 329-333, 2011.

[10] P. Mohanty, S. Panigrahi, N. Sarma, and S.S. Satapathy, "Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey", Journal of Theoretical and Applied Information Technology, vol. 13, pp. 14-27, 2010.

[11] Taranpreet Kaur, Dr. Krishan Kumar Saluja, Dr Anuj Kumar Sharma, "DDOS Attack in WSN: A Survey", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2016), vol. 4, pp. 131-140, 2016.

[12] Shital Patila, Sangita Chaudhari, "DoS attack prevention technique in Wireless Sensor Networks", Elsevier 7th International Conference on Communication, Computing and Virtualization 2016, vol. 79, pp. 715-721, 2016.

[13] Raksha Upadhyaya, Uma Rathore Bhatta, Harendra Tripathia, "DDOS Attack Aware DSR Routing Protocol in WSN", ELSEVIER International Conference on Information Security & Privacy (ICISP2015), vol. 78, pp. 68-74, 2016.

[14] Raksha Upadhyay, Salman Khan, Harendra Tripathi, Uma Rathore Bhatt, "Detection and Prevention of DDOS Attack in WSN for AODV and DSR using Battery Drain", 2015 Intl. Conference on Computing and Network Communications (CoCoNet'15), vol. 3, pp. 446-451, 2015.

[15] Varsha Nigam, Saurabh Jain, Dr. Kavita Burse, "Profile based Scheme against DDoS Attack in WSN", IEEE 2014 Fourth International Conference on Communication Systems and Network Technologies, vol. 5, pp. 112-116, 2014.