Prevention and detection of DDoS attack on WSN

Inzimam Ul Hassan[1], **Amandeep Kaur**[2]
M. Tech Scholar , Assistant Professor
Lovely Professional University , Lovely Professional University
Email – [1] inzimamulhassan@gmail.com , [2] amandeep3.kaur@lpu.co.in

Abstract: *The self-configuring type of network in which the sensor node are deployed in such a manner that they can join or leave the network when they want is known as wireless sensor network. The nodes start communicating with each other in order to transmit important information within the network. As this type of network is decentralized in nature, there are numerous malicious nodes which might enter the network. Due to the presence of such malicious nodes, the attacks can be triggered which are classified as active and passive types of attacks. The type of attack in which the raw packets are flood to the victim node is known as DDoS type of attack. It is an active type of attack. When the DDoS attack occurs in the network, it minimizes the lifetime of the network and also increases the overall energy consumption of the network. In order to detect the malicious nodes from the network which cause the DDoS attack, a novel approach is to be proposed in this research work.*

Key Words: *DoS, DDoS, WSN, MAC, IP.*

1. INTRODUCTION:

1.1 WIRELESS SENSOR NETWORK (WSN)

There are numerous sensor nodes deployed within a wireless sensor network (WSN) along with one base station in it. The sensor nodes are small sized devices which have very less power, and cost along with constrained memory, computational and communication resources. There are numerous spatially distributed autonomous sensors present within the network which Gather the information from their surroundings and pass it to the base station.

The nodes deployed within these networks collect the information from surrounding environmental areas. All the gathered information is transmitted to the base station present in the network which acts as a gateway amongst the sensor networks and the external environment. The storage capacity of base stations is very high and it also consists of numerous data processing capabilities which can be useful in the network [2]. The transmitting of important information which is received from the sensor nodes by the base station is its major task. This information can be accessed by the end user and can be utilized as per its requirement. Within the area of base station basically the sensor nodes are deployed which can form groups as per the requirement of the application.

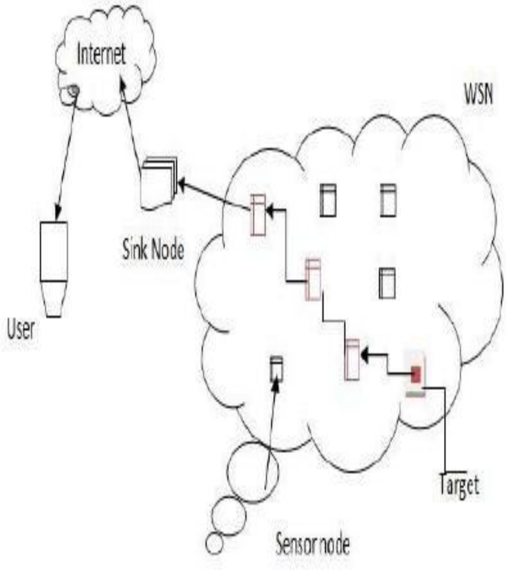


Fig 1 Traditional wireless sensor network [1]

1.2 Attacks in WSN: There are number of attacks in WSN some of them are given below:

1.3 Denial of Service (DOS) attack: There are various types of DOS attacks which can be triggered at different layers but the primary motive of these attacks is to temporarily make the network resources unavailable. If we talk about an example then at network layer it can result into homing or misdirection and at transport layer it can be performed by flooding. The complete programming of the sensors can be manipulated by the attackers. The attackers can be so influential that they can even place a false sensor in place of a legitimate sensor resulting the modification of whole circuitry.

1.4 Distributed Denial of Service (DDOS) 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. The secondary victims are those that are used to launch the compromised systems and primary victims are those that attack the services.

2. LITRATURE SURVEY:

MANIK LAL DAS and co-workers (2009) present a two factor user authentication protocol for WSN, which provides strong authentication, session key establishment, and achieve efficiency. The two actor user authentication protocol for WSN using only hash function. The two-factor user authentication protocol avoids many logged in users that have same login-id and stolen-verifier attacks, which are very well known threat for the password based system if it maintains verifier table at the sensor node. And also the two-factor user authentication protocol counter other attacks in WSN except the denial of service and node compromise attack.

H.WEN and co-workers (2011) detect the attack against node cloning. The attacker can easily launch the clone attack by adding on or mode nodes into the network by cloning captured nodes. Cloning attack can be a severe threat to the wireless sensor network (WSN). The authors follow the idea of the spatial variability characteristics of wireless channels and proposed a new lightweight method for clone node detection attack in WSN. The authors achieve fast detection and minimizing the packet transmission overhead without compromising the security requirements. The lightweight method can overcome number of problems in the conventional up-layer clone nodes detection approaches and serve as a purpose for replication nodes detection in WSNs.

G.Varaprasad, et.al, (2012) propose a secure Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP). In secure Energy Efficient Node Disjoint Multipath Routing Protocol the data packets are transmitted in a secure manner by using digital signature crypto system. The secure energy efficient node disjoint multipath routing protocol provides security using digital signature, which is generated by using the MD5 hash function and RSA algorithm. The security ensures the correctness of data, authentication and non-repudiation. The secure energy efficient node disjoint multipath routing protocol also defends data tempered or altered routing, selective forwarding, sink hole and byzantine attack. EENDMRP compared with the AOMDVRP, EENDMRP shows better result in terms of packet delivery fraction, energy consumption and end-to-end delay.

YONGSHENG LIU and co-workers (2012) proposed a novel PKC (public key cryptography) based broadcast authentication scheme using signature amortization for Wireless Sensor Networks (WSNs). Public Key Cryptography (PKC) is widely used for Broadcast authentication. Intensive use of PKC for broadcast authentication, however, is thought to be expensive to resource constrained sensor nodes. The PKC based broadcast authentication scheme using signature amortization for WSN employs only one digital curve digital signature algorithm (ECDSA) to authenticate all the broadcast messages. The overhead of the signature is amortized over all broadcast messages. The PKC based broadcast authentication scheme using signature amortization for WSN retains high security as strong as conventional PKC based broadcast authentication schemes. The PKC based broadcast authentication scheme using signature amortization for WSN overcomes defects of μ TESLA that is it does not require time synchronization, has an efficient public key distribution protocol and can achieve immediate authentication.

Varsha Nigam, et.al, (2014), has concluded that for working in critical conditions, WSN has proved out to be a good and reliable technology. The sensor networks can be deployed at various places such as war zones, buildings or traffic surveillance. If we talk about one major challenge in the use of wireless sensor networks then it can be the security issues. In this paper, authors have proposed a profile based protection scheme (PPS security scheme against DDoS (Distributed Denial of Service) attack. Flooding of excessive data is the major cause of this kind of attack because of which the bandwidth of the network is completely consumed by data delivery which affects the overall performance of the network. [8].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 PPS blocks the attack initiated by the attacker by checking it through profile based security scheme. A performance metrics can be utilized to evaluate the performance of the network. If the simulation results represent the same performance in case of normal routing and in case of PPS scheme, it means that the PPS scheme has worked with complete efficiency and shows 0% infection in presence of attacker.

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. This is prove to be economical and simple solution for different applications. The WSN have open nature that leads it to be affective for different security threats. In network, the information and sensor node information is compromised due to different security attacks such as black hole, wormhole attack, DDOS attack, etc. The goal of DDOS attack is to infect the network by the drainage of resource capability. Meaningless messages in large numbers are sent by the attacker to increase the network congestion and also degrade 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 [9], 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.

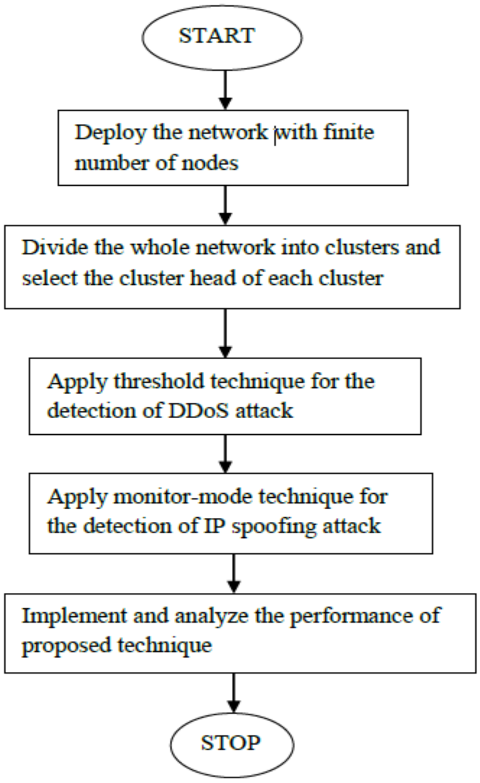
Raksha Upadhyaya, et.al, (2016), have analyzed that open nature of wireless sensor networks (WSN) results in more vulnerability to outside attacks. Different attacks such as denial of service, black hole and sink hole highly affect the overall output of the network. DDOS attacks the most dangerous attacks which greatly harm and hamper the complete working of the network. Distributed denials of service (DDOS) attacks are attacks that are launched by a set of malicious entities towards a node or set of nodes. In this paper [10], 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. Since a sensor network does not have any blacklist to detect malicious nodes therefore a shutdown method can be applied to ignore malicious node in the 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.

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 worm hole attack in order to disturb the overall functionality of network. When it is used in military and industrial applications the risks are more. The constraints in WSN are limited battery power, low capabilities of nodes etc. The challenge for researchers is to present a security model that will consider these constraints and provide security. 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. There are some weaknesses in WSN that results in that there sensor nodes are more vulnerable to most of the security threats. 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. But it has some disadvantages such as lacks in learning capabilities and based on single normal model which does not change over the time during detection. So, 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.

3. PROPOSED WORK:

An active attack that is responsible for dropping the data and control packets within the network is known as the selective forwarding attack. There is a minimization of performance of network in terms of various parameters when a malicious node is present within the network. The parameters such as energy consumption, throughput and delay define the performance of the network which can change as per the modifications made within the network. In this work, in order to recognize and remove the malicious nodes from the network, a technique has been proposed. On the basis of traffic analyzer and threshold values present within the network, there is a technique proposed. The central controller is chosen within the network depending on the trust values of the nodes. Depending on the data packets that are re-transmitted within the network, the trust value of the node is computed. There is a central controller node that registers each node according to IP, MAC address and the current data. The bandwidth required for communication related to the base station is assigned using the central controller node. Depending on the hop count and sequence number, a secure and efficient path is generated from sensor node to base station. The data is transmitted from the sensor node. Further the central node checks individually each node in a random manner. The nodes that have threshold unequal to the decided threshold value are to be detected and presented as malicious node within the network. For removing such malicious nodes from the network, a multipath routing method is presented here.


START
Deploy the network with finite number of nodes
Divide the whole network into clusters and select the cluster head of each cluster
Apply threshold technique for the detection of DDoS attack
Apply monitor-mode technique for the detection of IP spoofing attack
Implement and analyze the performance of proposed technique
STOP

4. CONCLUSION:

In this research work, it has been concluded that Wireless Sensor Network is the self-configuring network due to which some malicious nodes enter the network which are responsible to trigger active and passive attacks in the network. The DDoS attack is the Distributed Denial of Service attack in which the malicious nodes flood the victim with the raw packets. The technique of threshold will be proposed which detects and isolated malicious node from the network. The proposed improvement leads to increase network lifetime, throughput and reduce network delay.

REFERENCES

1. Sukhwinder Sharma, Rakesh Kumar Bansal, Savina Bansal,(2013) “Issues and Challenges in Wireless Sensor networks”, IEEE International Conference on Machine Intelligence Research and Advancement, vol 4, pp.58-62,.
2. M.H. Anisi, A.H. Abdullah, S.A. Razak (2011), “Energy-Efficient Data Collection in Wireless Sensor Networks”, Wireless Sensor Networks, vol. 3, pp. 329-333,.
3. Priyanka Goyal, Sahil Batra, Ajit Singh (2011), “A Literature Review of Security Attack in Mobile Ad-hoc Networks”, International Journal of Computer Applications, vol.9, pp.1115,.
4. M. Das (2009), “Two-factor user authentication in wireless sensor networks, “Wireless Communications, IEEE Transactions on, vol. 8, no. 3, pp. 1086-1090,.
5. H. Wen, J. Luo, and L. Zhou,(2011) “Lightweight and effective detection scheme for node clone attack in wireless sensor networks,” IET wireless sensor systems, vol.1, no.3, pp. 137-143,.
6. R. D’Souza, G. Varaprasad, et al.(2012), “Digital signature-based secure node disjoint multipath routing protocol for wireless sensor networks,” Sensors Journal IEEE, vol. 12, no. 10, pp. 2941-2949,.
7. Y. Liu, J. Li, and M. Guizani (2012), “Pkc based broadcast authentication using signature amortization for wsns,” Wireless Communications, IEEE Transactionson, vol.11, no. 6, pp. 2106-2115,.
8. Varsha Nigam, Saurabh Jain, Dr. Kavita Burse (2014) , “Profile based Scheme against DDoS Attack in WSN”, IEEE 2014 Fourth International Conference on Communication Systems and Network Technologies, vol. 5, pp. 112-116,.

9. Raksha Upadhyay, Salman Khan, Harendra Tripathi, Uma Rathore Bhatt (2015), "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,.
10. Raksha Upadhyaya, Uma Rathore Bhatta, Harendra Tripathia (2016), "DDOS Attack Aware DSR Routing Protocol in WSN", ELSEVIER International Conference on Information Security & Privacy (ICISP2015), vol. 78, pp. 68-74,.
11. Taranpreet Kaur, Dr. Krishan Kumar Saluja, Dr Anuj Kumar Sharma (2016), "DDOS Attack in WSN: A Survey", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2016), vol. 4, pp. 131-140,.
12. Shital Patila, Sangita Chaudhari (2016), "DoS attack prevention technique in Wireless Sensor Networks", Elsevier 7th International Conference on Communication, Computing and Virtualization 2016, vol. 79, pp. 715-721,.