A Novel Approach to Mitigate DDoS Attack Using Gateway Mechanism

Satvir Kaur[a], Gureshpal Singh[b], Baljinder Singh[c]
[a] Research Scholar, Beant College of Engineering and Technology, Gurdaspur, Punjab, India
[b] Beant College of Engineering and Technology, Gurdaspur, Punjab, India
[c] Beant College of Engineering and Technology, Gurdaspur, Punjab, India
[a]*satbirkaur019@gmail.com*

Abstract: Intelligent and economical sensors, connected to the network via wireless links and distributed in large quantities, offer unprecedented opportunities to monitor and control homes, cities and the environment. In addition, sensors connected to the network use a wide range of applications within the defence area, generating new features for recognition and surveillance and various tactical applications. Denial of service is one of the most terrible attacks is the cloning attack of the node, where the attacker captures the knot and extracts its secret information, create replicas and enter them in the network field other malevolent behaviour. To detect and mitigate this attack, this paper proposed a Gateway based technique.

*****

I. Introduction

A wireless device network (WSN) includes lots to an outsized range of low-power multi purposeful sensor nodes, operative among the unattended atmosphere, and having sensing, computation and communication capabilities. The essential of various components of a node beyond question are a device unit, ADC (Analog to Digital Converter), a CPU, electrical unit similar to a communication unit. Device nodes are micro electro-mechanical systems (MEMS) that develop a measurable a reaction to a general modification in some fitness like temperature and pressure. Device nodes sense and live the physical information within the space being monitored. The continual Associate in Analog signal perceived through the sensors is digitized by a digitizer and sent to controllers for additional process. Device nodes that are of tiny size, consume very low energy, are operated in high volumetrically densities, and can be autonomous and adjust towards the atmosphere.

Wireless device networks are significantly attention-grabbing in venturesome or wireless environments, or whenever a large number of device nodes must be deployed. The localization concern is very important wherever uncertainty regarding some positioning occurs.

The key characteristic of any WSNs includes:

1. Cross layer design
2. Mobility of nodes
3. Power consumption constraints for nodes using batteries or energy harvesting
4. Heterogeneity of nodes
5. Scalability to large scale of deployment
6. Chance to cope with node failures (resilience)
7. Simplicity of use
8. Capability to withstand harsh environmental conditions

II. Related Work

[1] Said that WSNs is an economical and trouble-free solution for a variety of applications. The open nature of WSN makes it defenseless against various security threats. Various security attacks, black hole, wormhole attack, DDOS attack, etc. it is possible to collaborate with the information and the sensor node in the network. The Distributed Denial of Service (DDOS) attack is a type of attack whose purpose is to interrupt the network by downloading the resource's capacity. The attacker not only sends insignificant messages to increase network traffic, but also degrades the life of the node and the network. In WSN, the life of the network is directly proportional to the capacity of the battery. In this way, the drainage of the energy of the battery directly degrades the life of the node. This work considered it a serious problem and designed a solution to overcome the problem of energy consumption due to DDOS attack. The Qualnet 5.0 simulator was used to simulate and evaluate the performance of the proposed solution for AODV and DSR routing protocols in WSN.

[2] Said that WSNs are likely to be vulnerable when they select the cluster head between sensor nodes. IDS cannot avoid it or act, but it can only detect it. IDS informs the controller to take the necessary measures when activating the alarms if an attack is detected, which is positive, but also involves a waste of resources and a waste of time in the detection process. Prevention must be carried out in the state of launch of the attack in order to reduce the waste of resources and the consumption of time. Initially, the attacker launches the attack to enter the selection of group heads (CH) that transmit control messages with false information, such as high energy & neighbour counting. The results of the experimental simulation work, to detect attacks at the basic level & improve network performance, to avoid the

attack in order to reduce the resource overload and to perform routing & aggregation of data resident in the WSN.

[3] Proposed that the WSNs is a large-scale network with dozens of hundreds of small devices. The use of WSN fields such as the army, health, the smart home has a large scale and its areas of use are increasing day by day. The WSN safe theme is an important research area & WSN applications have some important security shortcomings. The intrusion detection system is a second line of network security mechanism and is very important for integrity, privacy and availability. Intrusion detection in WSN is something other than wireless networking with no power restrictions, since WSN has some restrictions that affect the types of attacks and cyber security attacks. This paper is a survey that describes the types of attack of WSN intrusion detection approaches that oppose this type of attack.

[4] Studied and analyzed the impact of the jam on micaz specks running Tiny OS and explores ways to mitigate the impact. Interference is facilitated by disabling the detection of the carrier on the interference nodes. The interference attack is detected while monitoring RSSI and PDR on the receiver. Varying different parameters in the sender, such as power level, package size, distance with theoretical analysis

[5] Introduced a secure routing protocol for WSN, which is able to avoid DDoS attack on the network. In our methodology, we analyze the malicious nodes using the proposed algorithm and block that node from any other activity on the network. To protect the network, we use an intrusion prevention scheme, in which specific network nodes act as an IPS node. These nodes operate in their radio range for the region of the network and regularly scan neighbors. When the IPS node encounters a misconduct node that involves frequently sending messages other than UDP and TCP messages, the IPS node blocks the malicious node and sends the information to all the original sender nodes to modify its routes. All simulation work was done using NS 2.35. After simulation, the proposed scheme provides feasible results to protect the network from the DDoS attack. Performance parameters have been improved after the application of the security mechanism in an infected network.

[6] Said that with the advancement and innovation, one of the fundamental concerns nowadays is security. There are a few conceivable assaults on WSN, in DDOS assaults (Distributed Denial of Service), malignant nodes are adjusted to numerous assaults, for example, flood assaults, dark gaps and hot-opening assaults, to stop the general activity of the system. The dangers are considerably more prominent when one talk about military and modern applications. Besides, there are numerous confinements in WSN, for example, constrained battery limit, low bunch limit, and so forth. Showing a security demonstrates that thinks about these confinements and gives security is a noteworthy test nowadays. There are a few instruments proposed by scientists to recognize or shield against this DDOS assault.

[7] Said that specially appointed wireless systems are dynamic in nature. Ad-Hoc systems don't rely upon any default foundation. At whatever point correspondence is required by then, this system can be executed. In this article they talk about vampire assaults. Vampire assaults are anything but difficult to perform through the system and hard to distinguish. At that point they contrast the new technique and the current convention and Beacon Vector directing. What's more, they reach the resolution that the new convention is better, since it distinguishes and anticipates vampire assaults.

[8] Proposed a security conspire dependent on the profile (PPS assurance plot against Distributed Denial of Service (DDoS).This expansive number of assaults is flooding the measure of access pointless bundles on the system, and the width of Network transfer speed is devoured by the information dispersion systems are influenced, its primary goal is to imagine the impact of DDoS assaults on the system and recognize the hub or nodes that are influenced as far as system execution. is to check the profile of every node on the system and just the aggressor is a hub that overwhelmed superfluous parcels in the system, at that point PPS obstructed the assailant's execution The system is estimated dependent on execution measurements, for example, directing burden, execution, and so on. The reenactment results speak to a similar execution on account of ordinary directing and on account of a PPS conspire, it implies that the PPS plot is viable and indicates 0% disease within the sight of an assailant.

[9] Asserted that a DDoS is one of the harmful type of attack assaults. The constrained energy of the SNs is squandered and causes the loss of information parcels inside a system. A DDoS assault dispatches an organized assault by flooding goal nodes with false demands, along these lines exhausting their assets and compelling them to refuse assistance to genuine part nodes. In this investigation, the creators propose a message examination conspire for WSN. The strategy can identify vulnerabilities that are helpless against a DDoS assault. In addition, it can identify every one of the tradeoffs by assaulting messages transmitted through the sending nodes. The proposed technique is contrasted and other related conventions. The outcomes demonstrate that your technique can adequately identify and guard against DDoS assaults in WSN.

III. Architecture for Proposed Approach

Based on the above-related work, an observation is made that DDoS attacks are quite dangerous and need to be mitigated.

Therefore, this section shows the way to mitigate the DDoS attack using optimized Gateway Based Scenario. The following Flowchart illustrates the working of the mechanism.

Flowchart

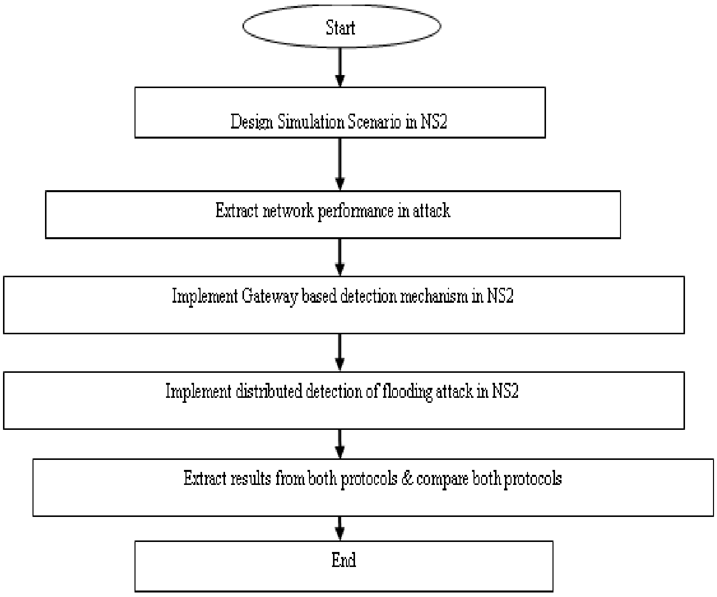
Start
Design Simulation Scenario in NS2
Extract network performance in attack
Implement Gateway based detection mechanism in NS2
Implement distributed detection of flooding attack in NS2
Extract results from both protocols & compare both protocols
End

Fig. 1. Proposed Flowchart

IV. Conclusion

One of the most alarming attacks in the WSN is the cloning attack of the nodes where the attacker takes the details of the node and collects their personal data, duplicates them and inserts them into the network field for further malicious activities. To detect and eliminate this type of attack, different detection techniques have been designed based on both static and mobile WSNs. Therefore, in this paper a proposal is given on the way to overcome DDoS attack using Gateway technique.

References

[1] R.Upadhyay, S. Khan, H. Tripathi, U. Rathore Bhatt, “Detection and Prevention of DDOS Attack in WSN for AODV and DSR using Battery Drain,” Intl. Conference on Computing and Network Communications (CoCoNet'15), 2015.

[2] S.Maidhili R, Karthik GM, “Intrusion Detection and Prevention Based on State Context and Hierarchical Trust in WSNs,” International Conference on Computer Communication and Informatics, Coimbatore, INDIA, 2018.

[3] O. Can and O. Sahingoz, “A Survey of Intrusion Detection Systems in WSNs,” IEEE, 2015.

[4] S. Rao, Deepak S and P. Pradeep, “Parametric Analysis of Impact of Jamming in WSNs,” IEEE, 2013.

[5] S.Nagar, S.S Rajput, A.K Gupta and M.C Trivedi, “Secure Routing Against DDoS Attack in WSNs,” 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT), 2017.

[6] T. Kaur , K. Saluja and A. Sharma, “ DDOS Attack in WSN: A Survey,” IEEE International Conference on Recent Advances and Innovations in Engineering, Jaipur, India, 2016.

[7] P.. Gosavi and B. Patil, “Draining Life from Wireless Ad –hoc Sensor Networks,” International Journal of Computer Applications (0975 – 8887) Volume 144 – No.9, June 2016.

[8] V.Nigam, S.Jain and K. Burse, “Profile based Scheme against DDoS Attack in WSN,” Fourth International Conference on Communication Systems and Network Technologies, 2014.

[9] A .Abidoye and I. Obagbuwa, “DDoS attacks in WSNs: detection and countermeasures,” IET Wireless Sensor System, 2018, Vol. 8 Iss. 2, pp. 52-59, The Institution of Engineering and Technology 2017.

[10] N. Shone and Q. Monnet “Predicting the Effects of DDoS Attacks on a Network of Critical Infrastructures,” IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, 2015.

[11] C.Kavitha, “Complete Study on Distributed Denial of Service Attacks in the Presence of Clock drift,” ICICES2014, Chennai, Tamil Nadu, India, 2014.

[12] V. Kansal and M. Dave, “Proactive DDoS Attack Detection and Isolation,” International Conference on Computer, Communications and Electronics (Comptelix) Manipal University Jaipur, Malaviya National Institute of Technology Jaipur & IRISWORLD, July 01-02, 2017.