IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Detection and Prevention of DDoS Attacks in WSN using Artificial Neural Network

Sumanjit Kaur[1*], Mohit Marwaha[2], Guresh Pal Singh[3]

[1*]Department of Computer Science and Engineering, Beant College of Engineering and Technology/ I. K. Gujral Punjab Technical University Gurdaspur, Punjab, India
[2]Department of Information Technology, Beant College of Engineering and Technology/ I. K. Gujral Punjab Technical University Gurdaspur, Punjab, India
[3]Department of Information Technology Beant College of Engineering and Technology/ I. K. Gujral Punjab Technical University Gurdaspur, Punjab, India

[*]*Corresponding Author: sumanjit2491@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 25/Jul/2018, Published: 31/July/2018

***Abstract*—** A wireless network with the advantages of sensing and processing information is referred to as a Wireless Sensor Network (WSN). It consists of a small sensor node with sensors, a battery, a microprocessor and a storage medium. It is an economical and simple solution for a variety of applications. The openness of wireless sensor networks makes it impossible to cope with various security threats. Several security attacks, black holes, wormhole attacks, DDOS attacks, etc., can jeopardize information and sensor nodes in the network. Distributed Denial of Service (DDoS) attacks are such attacks, the purpose of which is to destroy the network by exhausting resources. Attackers not only send worthless messages to increase network traffic, but also reduce the life of nodes and networks. In WSN, the lifetime of the network is proportional to the battery capacity. Therefore, depleting battery power directly reduces the life of the node. This research work has deal with the mitigation and prevention of DDoS attack by using Artificial Neural Network (ANN) as a classification algorithm. The simulation has been done in CLOUDSIM environment. The main of the work is to lessen the strength of attack with its prevention from reaching it to the victim with the anomaly detection system with the algorithm being proposed. Parameters, such as energy consumption, delay and PDR (packet delivery ratio) has been considered for the evaluation of the proposed work.

Keywords— WSN (Wireless sensor network), DDoS (Distributed Denial of service), CLOUDSIM, Energy consumption

I. INTRODUCTION

Wireless sensor networks can be considered as special types of ad hoc wireless networks, and there have been some proposals to address security in general ad hoc networks, but sensor networks have some additional problems that limit the applicability of these traditional security measures. Sensor networks are very limited in terms of local memory and computing power [1], so the security mechanisms of sensor networks cannot require each sensor node to store long-size keys to run very complex cryptographic protocols. Their power consumption is low, so sensor network protocols must focus on energy savings. Usually the sensor network consists of a large number of communication nodes, no global identification number, and may face easy node failures [2]. In a DoS attack, the attacker's goal is to make legitimate users unable to access the target. Sensor networks that do not have enough DoS attack protection may not be deployed in many areas. Node misconduct may include simple selfishness or lack of collaboration due to power savings, as well as proactive attacks and subversive traffic for DoS. There are two types of DoS attacks [3]:

- Passive attack: Selfish nodes use the network but do not cooperate to save battery life for their own communication; they do not intend to directly destroy other nodes.

Active attack: Malicious nodes cause network interruptions through partitioning and damage other nodes, while saving battery life is not a priority.

Table 1 describes typical DoS attacks and corresponding defense strategies [4]:

Table 1: DoS attack in sensor network

DoS attacks	DoS attacks Defense strategy
Radio interference	Use spread-spectrum
Physical tampering	Make nodes tamper-resistant
Denying channel	Use error correction code
Black holes	Multiple routing paths
Misdirection	Source authorization
Flooding	Limit the connections

Attacks that are not detected by existing available detection solutions are called unknown (zero-day) attacks. The ranges of attacks that can be performed on networks are as broad as the spectrum of constructive technology itself [5]. This paper deals with a specific category of attacks identified as Distributed Denial of Service (DDoS) attacks. Distributed Denial of Service (DDoS) attacks are a scaled form of DoS attacks where multiple attack are employed in a coordinated fashion to form an attack network for attacking a specific target. DDoS attacks are catastrophic particularly when implemented to extremely sensitive targets such as Critical-Information Infrastructure [6].

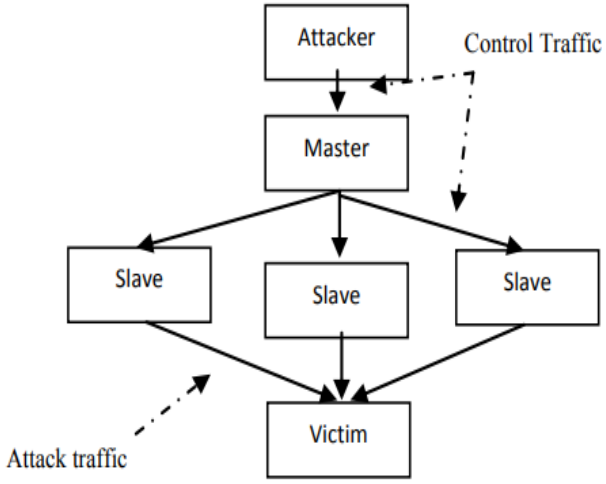

Figure 1: DDoS attack in WSN

So, in proposed work Artificial Neural Network will be used for prevention from DDoS attack occurring in the network [7]. The results have been evaluated in CLOUD SIM environment using parameters given as energy consumption, PDR and delay.

Section I contains the introduction of the work, Section II contains the proposed architecture, Section III contains the results and discussion Section IV contains the conclusion of the work.

II. PROPOSED ARCHITECTURE

This research work has studied the detection of known and unknown DDoS attacks of high and low rates as opposed to detecting known attacks in real time only and preventing the attacking packets from reaching the target whereas allowing genuine packets to get through. The strength of the attack has been reduced and is prevented from reaching to the victim using anomaly detection systems using proposed algorithm. Neural network is used for training, deploying and testing the proposed solution in a physical environment in CLOUD SIM.

The methodology considered to simulate the work is defined below in the form of flowchart with the explanation:

Step 1: Deploy Network using length and width.
Step 2: Find DDoS Attack in the network.
Step 3: Apply Neural Network for prevention of DDoS attack using detectors that will prevent the attack by checking the abnormalities.
Step 4: Check the system performance of the network using metrics energy consumption, PDR and delay.

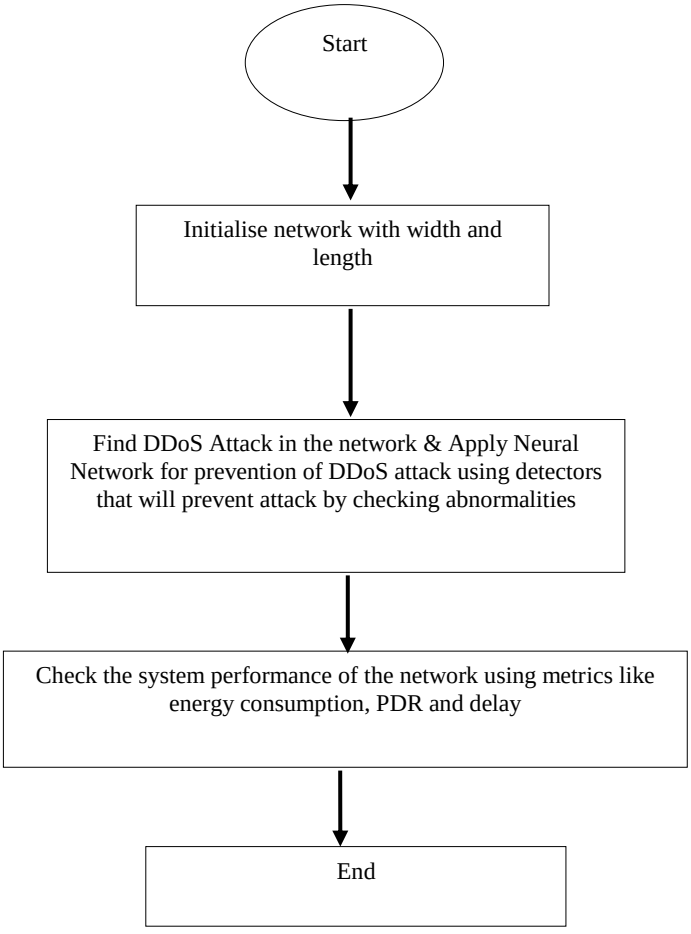

Figure 2: Proposed Architecture

III. RESULTS AND DISCUSSION

This section defines the results obtained after the simulation of the proposed work. To compute the results, parameters such as energy consumption, delay and PDR (Packet delivery ratio) are considered.

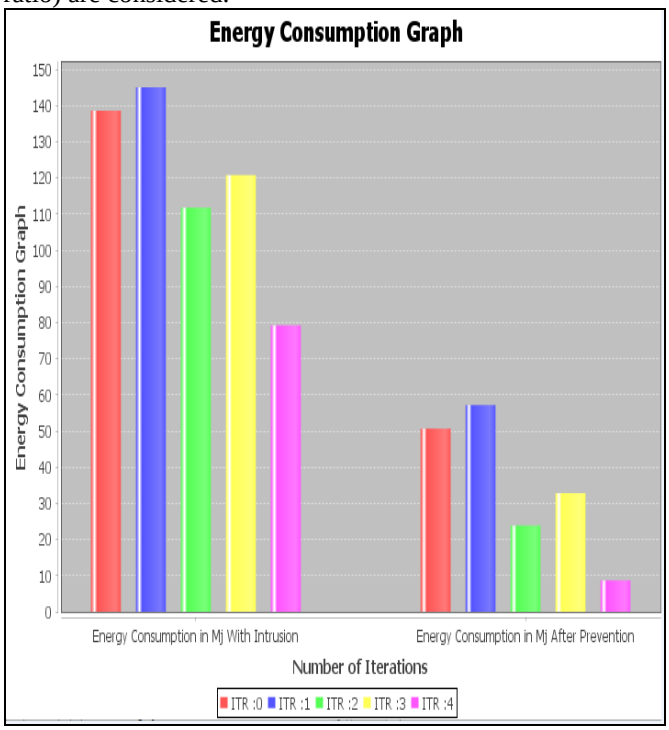

Figure 3: Energy consumption computation

The above figure represents the graph plotted between energy consumption rates with respect to number of iterations. The energy is measured in mJ in the presence of intrusion and after applying the prevention algorithm. When Prevention algorithm is applied the energy consumption rate is reduced as shown in figure above.

Table 2: Energy consumption with and without prevention

Number of iterations	Energy consumption with intrusion	Energy consumption without intrusion
1	139	50
2	145	58
3	110	25
4	120	32
5	80	9

The average value of energy consumption obtained for the without prevention and with prevention algorithm are 118.8 and 34.8 respectively. Thus there is a decrease in the energy consumption arte when prevention algorithm is applied.

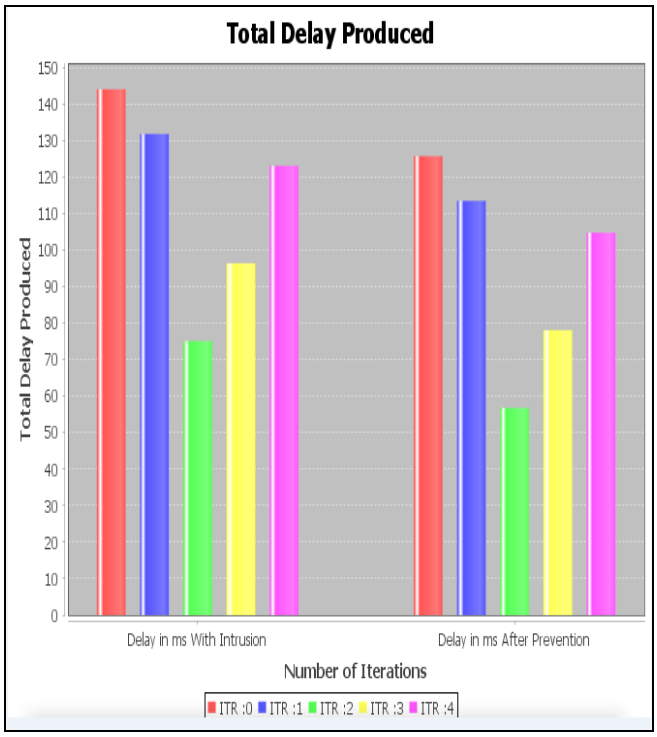

Figure 4: Delay computation

The above figure represents the total delay produced by the nodes within the network in case of attack and when prevention algorithm is applied in the network.

Table 3: Delay with and without prevention

Number of iterations	Delay with intrusion	Delay after prevention
1	142	125
2	131	112
3	72	55
4	95	78
5	122	105

The values of delay obtained for five iterations are listed in table above. The average value of delay obtained with intrusion and with prevention are 112.4 ms and 95 ms respectively. Thus there is an reduction of 15.56% in the delay value when prevention algorithm is applied in the network.

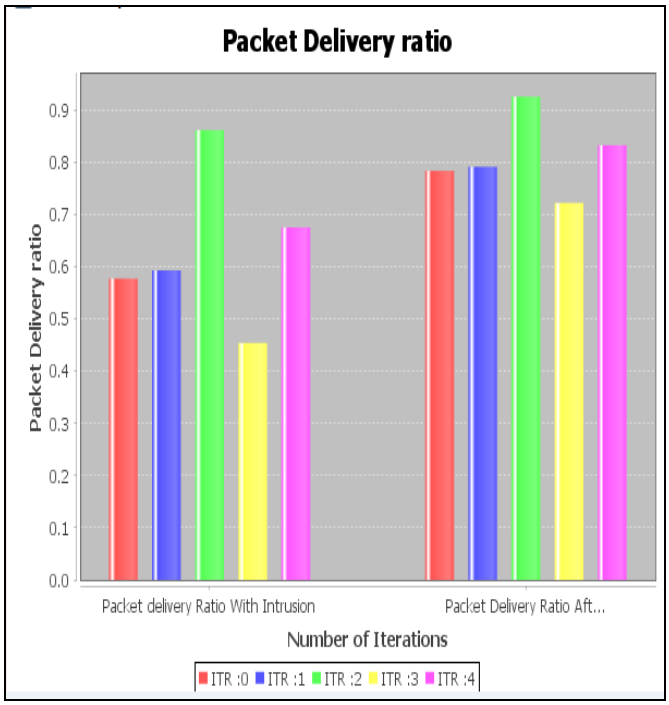

Figure 5: PDR Computation

The figure defines the PDR value obtained for the network with intrusion and with prevention algorithm for the proposed work. X- Axis defines the number of iterations and y-axis defines the PDR value of the proposed work.

Table 4: PDR with and without prevention

Number of iterations	PDR with intrusion	PDR without intrusion
1	0.58	0.78
2	0.59	0.79
3	0.85	0.92
4	0.45	0.72
5	0.67	0.82

The values of PDR obtained for five iterations are listed in table above. The average value of PDR obtained with intrusion and with prevention are 0.628 and 34.46 respectively. Thus there is an increment of 98.18 % in the PDR value when prevention algorithm is applied in the network.

IV. CONCLUSION

Wireless sensor networks are rapidly evolving due to their cost-effective solutions for sensitive and remote applications such as military, medical and environmental applications. But because of the limitations of range, memory, processing and power, collecting important remote data from wireless sensors is really challenging. The use of ad hoc networks and radio waves for data transmission also increases the chances of attackers attacking such networks. Various solutions have been proposed in the past to combat WSN attacks in wireless sensor network security. In the network, DDoS threats are a major problem that causes serious attacks between servers and users. The situation of Internet attacks is increasing in a direction of decentralization and mutual orientation. Attacks on the Internet consume a lot of resources; creating a victim host cannot accept a normal network request and occupy a set of bandwidth, resulting in a large loss of network economy. Identifying the exact signature of an attack is not easy, and an intrusion detection system is a key module to ensure network and system security. In this research work, detection and mitigation of DDoS attack has been considered. ANN has been applied for the prevention using detectors that has prevented the attack by checking the abnormalities. For the computation of the performance, parameters such as energy consumption, PDR and delay has been considered. average value of energy consumption obtained for the without prevention and with prevention algorithm are 118.8 and 34.8, The average value of delay obtained with intrusion and with prevention are 112.4 ms and 95 ms and The average value of PDR obtained with intrusion and with prevention are 0.628 and 34.46 respectively.

ACKNOWLEDGMENT

I, Sumanjit Kaur, would like to thank my Guides Mr. Guresh Pal Singh, Associate Professor and Mr. Mohit Marwaha, Assistant Professor who have been a great source of inspiration and provided their right suggestions in preparing this paper.

REFERENCES

[1] I.U. Hassan, A. Kaur, "Prevention and Detection of DDoS Attack on WSN," International Journal of Research Culture Society, Vol.2, Issue.2, pp. 245-249, 2018.

[2] S. Nagar, S.S.Rajput, A.K. Gupta, M.C. Trivedi, "Secure Routing against DDoS Attack in Wireless Sensor Network," In Proceedings of the IEEE International Conference on Computational Intelligence & Communication Technology (CICT), pp. 1-6, 2017.

[3] P. Pandey, M. Jain, R. Pachouri,"DDoS Attack On Wireless Sensor Network: A Review," International Journal of Advanced Research in Computer Science, Vol.8, Issue.9, pp. 227-229, 2017.

[4] S. Dhuria, M. Sachdeva,"Detection and Prevention of DDoS Attacks in Wireless Sensor Networks," in Networking Communication and Data Knowledge Engineering , Perez G., Mishra K., Tiwari S., Trivedi M. (eds), Springer, Singapore, pp. 3-13, 2018.

[5] K. Kaushal, V. Sahni, "Early Detection of DDoS Attack in WSN," International Journal of Computer Applications, Vol.134, Issue.13, pp. 14-18, 2016.

[6] R. Upadhyay, U.R. Bhatt, H. Tripathi, "DDOS Attack Aware DSR Routing Protocol in WSN," International Conference on Information Security & Privacy (ICISP), pp. 68-74, 2016.

[7] S. Faizan, Z. Mushtaq, I. Rashid, "DDOS Attack in WSN: A Survey," International Journal of Computer Science and Mobile Computing, Vol.6, Issue.6, pp. 351-353, 2017.
[8] A.P. Abidoye, I.C. Obagbuwa, "DDoS Attacks in WSNs: Detection and Countermeasures," IET Wireless Sensor Systems, Vol.8, Issue.2, pp. 52-59, 2017.
[9] I.U. Hassan, A. Kaur, "Literature Review on Prevention and Detection of DDoS Attack," International Journal of Computer Engineering and Applications, Vol.12, Issue.4, pp. 260-266, 2018.
[10] S. Patil, S. Chaudhari, "DoS Attack Prevention Technique in Wireless Sensor Networks," In Proceedings of the ELSEVIER International Conference on Communication, Computing and Virtualization (CCV), pp. 715-721, 2016.
[11] S. Deol, L. Kaur, "Review On Detection and Prevention Schemes for Flooding Attack in WSNS," International Journal of Advance Research, Ideas and Innovations in Technology, Vol.8, Issue.2, pp. 1195-1197, 2017.
[12] S.S. Sahu, M. Pandey,"Distributed Denial of Service Attacks: A Review," International Journal of Modern Education and Computer Science, Vol.6, Issue.1, pp. 65-71, 2014.

Authors Profile

Sumanjit Kaur received the B. Tech. degree in Information Technology from Beant College of Engineering and Technology, Gurdaspur in 2013. She is currently pursuing M. Tech(CSE) from the same college under IKG Punjab Technical University, Jalandhar, Punjab.

Mohit Marwaha is an Assistant Professor in Department of Information Technology in Beant College of Engineering and Technology, Gurdaspur, Punjab. He did B. Tech(IT) and M. Tech(CSE). He possesses 10 years of teaching experience. His main research work focuses on Cloud Computing, Mobile Cloud Computing.

Guresh Pal Singh is an Associate Professor and Head of the Department in Department of Information Technology in Beant College of Engineering and Technology, Gurdaspur, Punjab. He is an M. Tech and currently pursuing Ph. D. He possesses more than 20 years of teaching experience. He has worked as teaching faculty in many reputed institutions in India. His work is published and cited in reputed journals and conferences. His main research work focuses on mobile ad hoc network (MANET).

