July – August 2020
ISSN: 0193-4120 Page No. 416 - 421

Distributed Denial of Service Attack Detection using Secure Neuro Fuzzy based System in Wireless Sensor Network

Pankaj Kumar Sharma
Assistant Professor, Department of CSE
Women Engineering College Ajmer, India
pankaj.gmeca@gmail.com

Dr.Uma Shankar Modani
Associate Professor, Department of E&C Engineering
Engineering College Ajmer, India
drusmodani@ecajmer.ac.in

Article Info
Volume 83
Page Number: 416 - 421
Publication Issue:
July - August 2020

Article History
Article Received*: 06 June 2020*
Revised*: 29 June 2020*
Accepted*: 14 July 2020*
Publication*: 25 July 2020*

Abstract
Wireless Sensor Networks (WSNs) comprise of huge number of sensor nodes for collecting the data and information which are sensitive for a particular application. Sensor nodes have restricted capabilities in terms of processing power, memory and battery life. Apart from limited capabilities of WSN , security is a major challenge as there could be a possibility of various type of viable attacks on the network, among which discussion on DDOS is vital. Distributed-Denial of Service(DDOS) is a cumulative term that contains various attacks that may affect the network by spreading the request message, dropping the packets originating from real source , degrade the overall performance of network. Threat is even more when military and industrial applications are involved.
To present a security critical solution that address these obstructions is a key challenge nowadays. There are lots of interesting methods which are implementing by researchers to identify or protect the network from DDOS attack, review of which is presented here in this paper on basis of suitable parameters. We have also presented a novel solution which of are compared with techniques belong to similar category.

Index Terms—Wireless Sensor Networks (WSNs), Sensor Nodes, Security, DDOS attack obstruction.

I. Introduction

WSN is a formation of tiny sensor nodes . These nodes are employing in many appeals such as farming, health, home, manufacturing, and armed forces for supervising and collection of data. The major convenience wireless sensor network is that the deployment of the sender node is easy in despotic environments. Along with ease of deployment there are few restraints associated that includes restricted battery power, low capacity of nodes, Hostile Environment, Limited Computational power etc. Additionally the region for formation of WSNs could be a public spot, where attacker can acquire sensor nodes and capture sensitive data. Further because of failures of energy a few nodes may demise, or new nodes can connect to the network. Due to various restraints in wireless sensor network, the typical security methods cannot be implemented conventionally therefore more systematic security approaches are eagerly awaited

II. TYPES OF DDOS ATTACK

DDOS intrusion have three main type as shown in Fig 1.

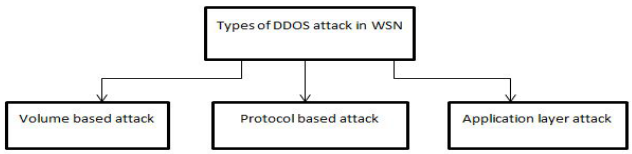

Figure 1. Types of DDOS

July – August 2020
ISSN: 0193-4120 Page No. 416 - 421

1) Attacks based on Volume:-This type of intrusion comprises of Internet Control Message Protocol floods, user datagram protocol floods and other spoofed packet attacks. The major aim of the attacker is
to ingest the transmission capacity of the area of victim. The volume of the irruption is compute in bits per second (bps).

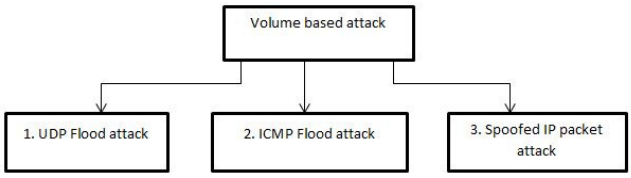

Figure 2. Types of volume based attack in DDOS

2) Intrusion situated on Protocol:- circulation of information at the fixed interval of time, fractioned packet irruption, clink of death etc. are included in these category of intrusion. The intruder is entered into the network of real resources like firewall. The value of the intrusion is computed in Packets per second.

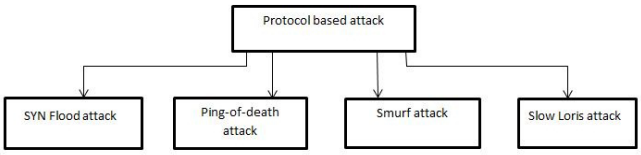

Fig. 3. Types of protocol based attack in DDOS

3) Application layer based attack: - These attacks are also combination of attacks such as Zero-day attack, Slow Loris etc. Mainly, attackers target to the Apache, Windows vulnerabilities.

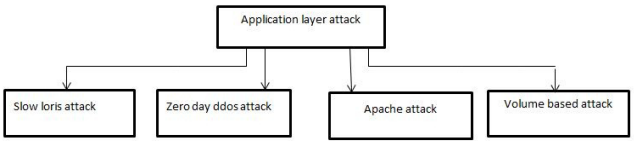

Fig. 4. Types of application layer based attack in DDOS

III. RELATED WORK

Lot of research has been carried out the efforts to protect WSN from DDOS attack. Now, we will look into various security approaches to secure against DDOS attack in WSN.
In paper [3] of Sang Min Lee et al., the distributed denial of service intrusion is perceived by employing a proposed prototype for enhanced traffic matrix. It comprise the enhancement of substructure an generic method, fabrication of traffic scheme and prediction of fluctuation. On the initial phase, there are three explores criterion are enhanced by generic method. The detection parameters subsist that are Framework range, window range based on fragmented data and trace assessment. When these elements are enhanced and achieve maximal perceive range, the presented prototype will become appropriate for the relative network domain. In the next phase, a traffic grid developed through sensing originator IP code deriving out of an inflowing transit spate and adopting a refined hash function spot the data packets to the traffic grid. In this paper, a fragmented data packet occupying window range is applied which is rather than time occupying window range for reducing the estimation aloft and by applying the distinct hash methods, the clashing of hash are evaded.GA has setup the traffic form range and the count of data files for single traffic form in this step. Now variation has evaluated by applying the traffic grid in the closing step. The variation in DDoS raid is less due to dissolvability in DDoS attacks but regular traffic is of a huge fluctuation. Afterwards, it can conclude whether inbound traffic is normal by analysing the fluctuation which was computed and a threshold rate established by the generic algorithm. Eventually, the prospective detection prototype produces vigilant at the time of detection of DDoS irruption Or else, the last two final phases are emphasized constantly.
In paper [4] A Novel Trace back Algorithm is proposed algorithm which have IP header of 25 bit slot consist Types of Service field have 8 bits slot, Identification field have 16 bits slot and reserved flag have 1 bit slot. Every fraction collects in to a packet through a sequence number and checksum and every sequence number of 8 bits. The sequence number of 8 bit is attached to the carried 8 bits to reset the packet through the re-establish point. Certainly addition of 8 bit checksum is done for delusion domination. There are, four different markings are possible through every device for a individual
origin IP and they are computed correctly afore the packet enter, an arbitrary indicating is elected from these calculated random possibilities for each packet to be marked. IP re-establish on the receiver side take place in two states
1. State of mark recognition 2. State of recovery of address
In the first state, domination field is evaluated to ensure that router is indicated the packet or not. Affinity issue should not be arises due to use of restrained flag field. The insignificant and incongruous checksum values of packets will be disposed at the time of restore operation. Therefore yet the joining router is destructed by intruder, it will no impact on the IP restore. The process of address restoration is achieved if the packet is indicated.
In this paper [5] Dynamic Solution for identify Denial of Service Attacks emphasis on cNodes that is accountable as detecting attacks in wireless sensor networks. At every cluster, there are number of sensor nodes that is N that appoint a controller node of cluster head by utilizing Low-energy adaptive clustering hierarchy (LEACH) Protocol. Afterward it selects some nodes that are denoted as K amid N that are appointed a cNodes. To implement that alternate an inducer of arbitrary number is employed to obtain a group of arbitrary numbers and a method that evaluate the ID of node equate to these arbitrary numbers is evolved. For producing those numbers, a Multiplicative Linear-Congenital Generators

July – August 2020
ISSN: 0193-4120 Page No. 416 - 421

(MLCG) is used in the next step another set is defined or selected K amid the K nodes which has procure via MLCG and the evolved method. Those K nodes which have the most surplus vitality that can implement network traffic analysing function. The motive of this resolution is to contribute to appoint at fixed interval these supervisor nodes in form to elude vitality consumption and for decreasing the probability of perception of these nodes by the intruders. At every interval of time there are variant set of controller nodes, a group head and sensing nodes present in a clutch. The proposed model has the method as follow:

Network is organized within clutches using Low-energy adaptive clustering hierarchy (LEACH) protocol as well as appointed a clutch superintendent in every clutch. The dynamic procedure is implement that designated the group of controller nodes in every clutch. The perception

procedure Implemented which could be detected whole intrusion execute on distinct kind of nodes in the clutch.

1) Formation of the network (clustering method):

LEACH the initial clustering method which has intended for designing assemble of sensing element in our network system and to select the CH present in all clutches and which produces balance of energy utilization by a random rotation of CHs and it permit to distribute the energy among all the sensors of the system.

2) Election of Nodes:

An arbitrary number provider of Multiplicative Linear Congenital Generator type is employed for elect the of controller nodes in each cluster. This generator is employed to obtain a extensive time of interval and to contain suitable arbitrary properties that enable eluding to choose the identical nodes at every poll of supervisor. As those numbers are produced from 0 to a number m, an algorithm is needed for the nomination of controller nodes that will equal to every arbitrary number produced to single node ID in the network.

In this paper [6] when an attack is occurred on sensor nodes of WSN, the agent-based attack perception and self-rehabilitation approach will observe the damaged point and perform self-rehabilitation. This method contains three stages are peculiarity perception, peculiarity conclusion and peculiarity rehabilitation. From nodes sensor data packet is supervised by handler of associate point if there is any anomaly intrusion, the handler of supervisor of clutch for min consistent outcome based on results that has provided by handler of associate point. If there is any actual intrusion then supervisor of clutch produce rehabilitation directives.

In this paper [7] perception of Distributed Denial of Service intrusion stand on Network Chaos concept and divination of congestion, there are some sequences of period of time prototype like “autoregressive integrated moving average”, “autoregressive fractionally integrated moving average” and etc. are employed for analysing and forecasting uniformity evaluation on network traffic proves that signals are passed at lower frequency by LPF and multiplexing can produce more desirable predictability. Although there may be large prediction error caused by, the bursty network traffic. Thus the sequences of period of time prototype should be comparatively fixed. Network traffic divination traffic divine drift intermittently.Things in the future underneath the counselling. Network rush prototype is arranged into two section. Conventional traffic prototype and current traffic prototype. Entire system is checked out when the congestion of the transmission of data and go on messages.

Step1:Packets are collected of network and information is proceed in fixed interval of time.

Step2:Pre-process network traffic by accumulatively moderating it.

Step3: The network congestion is divined through AR prototype.

Step4: Divination delusion is perceived.

Step5: The anomalous traffic is perceived by inspecting divination delusion depend on chaos theory.

Step 6: A competent neural network is employed to perceive the DDoS intrusion. For improvement of the efficiency of perceived, perceive neural networks are employed. The back-propagation method employs managed understanding to network to compute then the misconception is deliberated. Misconception is referred to the distinction of definite and assumed out comes. The objective of this method is to minimize that delusion, till the practicing data has learnt by the artificial neural network

In this paper [8] to perceived denial of service intrusion there a strategy is employed that is strong intensifying double verification of the utilization and it has employed following process:

1) A tree is named as merkle hash tree is manipulated for Lightweight pre-authentication. The gateway node is formed the tree in start-up state and applying in sign in or verification state to execute initial verification by exhausting single hash process, that able to block intruder acting denial of service intrusion as well as organize rigid restriction on entry of intruder in the network.

2) Confidential parameters are illustrated for sensor nodes. Conventional dispense rate between entry node and other sensor point form prior strategy undefended toward a form of intrusion induced through sensor point apprehend. The presented method categorizes the confidential rate for every sensor point, that is able defused this kind of secret effluence while retaining the attributes of two factor verification

A. Starting State

B. State of Registration

C. State of sign in or verification

D. State of innovation of Password

In this paper [9] curbing distributed denial of service intrusion through traffic filtering, an authentic node will spread the packets in a usual manner whereas malicious node will forward traffic viciously in a small period of time. The dos attack will curb by traffic filter through acquiring mitigation procedure. When the traffic rate drops below a conclusive point, compensation arise when they get some possibility to transmit

July – August 2020
ISSN: 0193-4120 Page No. 416 - 421

the traffic in a normal way. It imply that their traffic rate is improved the number of packets that are coming from invaders whose traffic rates have dropped, packets from the nodes which flow rate have been compensated and the packets from authenticated nodes are dispatched to the base station.
In this paper [10] to perceived distributed denial of service intrusion a strategy is used is a Profile based wireless sensor network, The entire network operations are superintend through profile based protection scheme (PPS). When the black hole attack is raised and adversarial device dispatch no fraction of data, rules situated on IAT auditing cannot discern an Incursion as no fraction of data report and IAT are not seized any value. Thus, auditing nodes should evaluate the count of information perceived from a certain origin node in a time intermission of a provided length (PRR) and IAT. Although rules based on IAT let on early anomaly determination but they have higher erroneous positive rate, and so the quality of link is unpredictable in opaque or open networks. PRR has analysed the lower erroneous positive rate, but it has determination lag. Forwarding nodes may be monitored assessment of IAT as well as PRR.

IV. PROPOSED SOLUTION

Distributed denial of service attacks are not new, but remain a major security challenge for detecting and preventing in the wireless sensor networks. We design the new secure protocol using Neuro fuzzy system with help of anomaly and misuse detection system. At first, our method applies zero knowledge protocol (ZKP) for verifying the legitimacy of the sensor nodes and then explore the explore the relationship between flow correlation coefficient and the length of flows of the traffic packets in the traffic optimization method. After traffic optimization in the Neuro fuzzy based detection model is proposed to detect and classify the different types of DDOS attacks and by proposing fuzzy based defence strategies with advanced decision making system in the new protocol in the wireless sensor network. The proposed method can characterizes regular network traffic of a service in the traffic optimization matrix to minimize the network congestion as well as hash collusions in the networks. Additionally energy efficient clustering based network model is utilized in order to make the detect the energy harvesting nodes in which it improves the throughput and reduces the latency and traffic congestion. we demonstrate optimized trade-off relationships between resiliency against compromised nodes and improves scalability of system

V. RESULTS AND OUTPUTS

The Network Simulator (NS2) is applied for simulation of proposed architecture. The IEEE 802.11 MAC layer is used for communication. AODV routing Protocol is used in the simulation. The simulation parameters are given in table 1.

Table 1. NS-2 Parameters

Channel type	Channel/ WirelessChannel
Radio-propagation model	Propagation/ TwoRayGround
Network interface type	Phy/ WirelessPhy
MAC type	Mac/802_11
Interface queue type	Queue/ DropTail/ PriQueue
Link layer type	LL
Antenna model	Antenna/Omni Antenna
Max packet in ifq	50
Number of mobile nodes	30
Routing protocol	AODV
X dimension of topography	600
Y dimension of topography	600
Time of simulation end	100.0
Traffic Source	CBR

Implemented method is compared with the PID-DDOS AND CS-DDOS detection technique. The performance is measured primarily based on performance metrics like PDR ,consumption, average delay, efficiency, loss, and routing overhead.

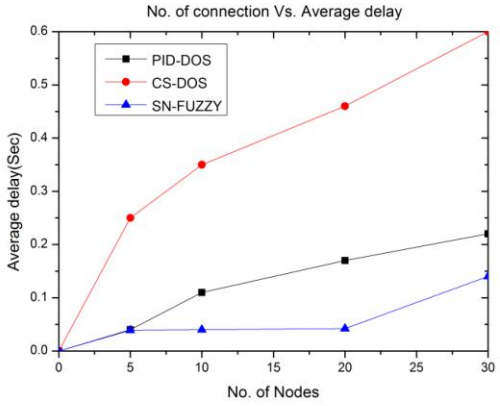

Figure 5. No. of connection Vs. Average delay

July – August 2020
ISSN: 0193-4120 Page No. 416 - 421

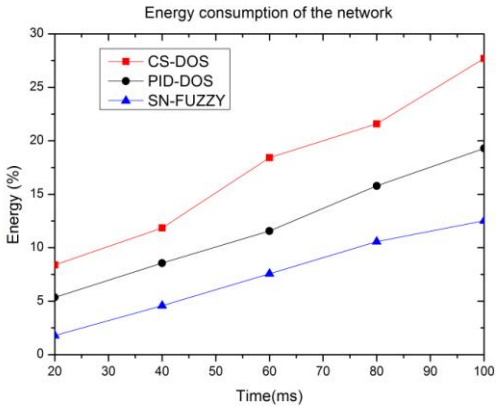

Figure 6. Energy consumption of the network

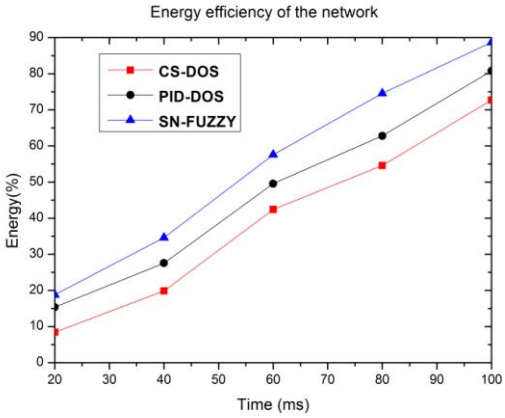

Figure 7. Energy efficiency of the network

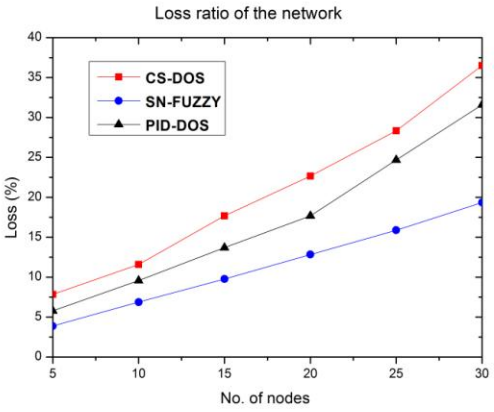

Figure 8. Loss ratio of the network

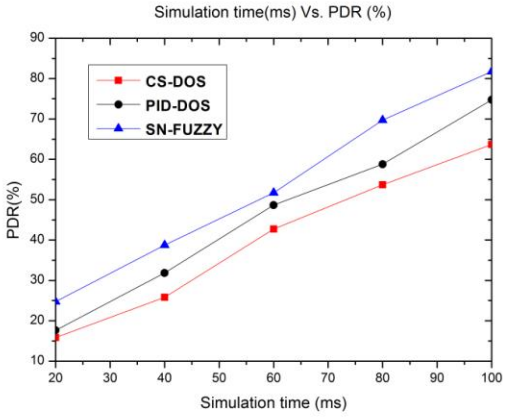

Figure 9. Simulation time(ms)Vs.PDR(%)

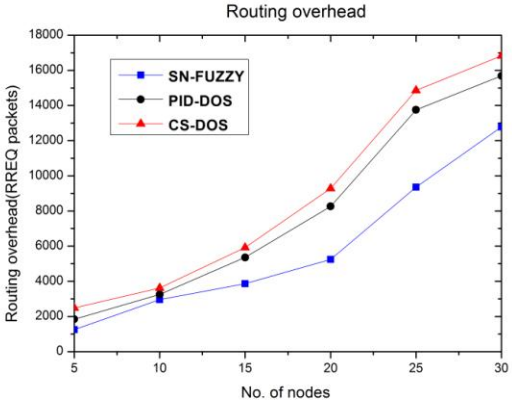

Figure 10. Routing overhead

VI. CONCLUSION

Wireless Sensor Network is exposed to vast variety of security attacks. Denial of service attacks require lesser effort to launch in WSN. In this paper we have discussed various protection principles related to attacks that are probable in WSN. Many security methods are available for WSN security, but it is still exposed to so many DDoS attacks. we have design a secure neuro fuzzy based protocol for detecting and preventing the distributed denial of service attack. Simulations and comparison graphs are showed that the performance of proposed protocol is better from recent methods.

REFERENCES

[1] Taranpreet Kaur, Dr. Krishan Kumar Saluja and Dr Anuj Kumar Sharma, “DDOS Attack in WSN:A Survey”, in IEEE International Conference on Recent

July – August 2020
ISSN: 0193-4120 Page No. 416 - 421

Advances and Innovations in Engineering (ICRAIE-2016), December 23-25,2016, Jaipur, India.

[2] Monika Malik and Dr.Yudhvir Singh "A Review: DoS and DDoS Attacks" in International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June- 2015, pg. 260-2656

[3] Sang Min Lee, Dong Seong Kim, Je Hak Lee and Jong Sou Park , "Detection of DDoS attacks using optimized traffic matrix," Computers and Mathematics with Applications 63(2012) 501510,pp. 216-220

[4] V.K. Soundar Rajam and Dr. S. Mercy Shalinie, "A Novel Traceback Algorithm for DDoS Attack with Marking Scheme for Online System," in IEEE ICRTIT-2012, pp. 407-412

[5] M.Guechari, L.Mokdad, and S.Tan, "Dynamic solution for detecting denial of service attacks in wireless sensor networks", IEEE International Conference communicationsICC12,Ottawa,Canada,June 2012, pp. 173-177

[6] Ting SUN and Xingchuan LIU, "Agent based intrusion detection and self-recovery system for wireless sensor networks" , IC-BNMT IEEE 2014, pp. 206-210

[7] Anjali. M, " Detection of DDoS Attacks based on Network Traffic Prediction and Chaos Theory," (IJCSIT)International Journal of Computer Science and Information Technologies, Vol. 5 (5), 2014, 6502-6505

[8] FeiWang, Yujun Zhang, Yongjun Xu, Lin Wu and Boy Diao, " A DoS-Resilient Enhanced Two-Factor user Authentication Scheme in Wireless Sensor Networks," ICNC 2014,pp. 1096-1102

[9] Sonali SwetaPadma sahu, Puja Priyadarshini and Saurabh bilgaiyan, "curbing distributed denial of service attack by traffic filtering in wireless sensor network" IEEE 33044 5th ICCCNT - 2014 July 11 - 13, 2014, Hefei, China.

[10] Nigam, Varsha, Saurabh 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,pp. 112-116

[11] Hongbin Luo, Zhe Chen, Jiawei Li, Athanasios and V. Vasilakos, " Preventing Distributed Denial-of-Service Flooding Attacks with Dynamic Path Identifiers, IEEE Transactions On Information And Forensics Security, DOI 10.1109/TIFS.2017.2688414