AN EFFICIENT SUPERVISED LEARNING APPROACH TO MITIGATE DDOS THREAT IN MANET

Rashid Rafiq Shah[1], Dr. Monika Sachdeva[2]

[1]Dept. of Computer Science and Engineering, I.K. Gujral Punjab Technical University kapurthala road Jalandhar-144603, india.
[2]Head of the Dept. of Computer Science and Engineering, I.K. Gujral Punjab Technical University kapurthala road Jalandhar-144603, India.

Abstract

The proposed work deals with the sensor network security in which the mitigation of the attack takes place using optimization and machine learning process. The back propagation neural network is used to detect the attack scenario and the optimization used is the moth flame optimization in which the effect of DDOS will be mitigated in terms of the network performance. The neural process will train the network in an iterative manner so that if there is any malicious activity occurs then it will detect and based on that the mitigation is performed. In the proposed approach the DDOS effect that we have considered is the flooding attack in which the performance of the network is evaluated in terms of overhead consumption, legitimate traffic comprises of alpha values and no. of packets per second are evaluated. From the simulations the proposed approach is well suited to perform detection and mitigation process up to that extent that the network will get stable with high network lifetime and low packet losses. So when the system knows that the flooding of the packets are increasing the overload on the nodes which acts as a server to communicate to the application units, then the system will exceeded the sessions of sending the packets which shows that the DDOS is occurred in the network or system. The proposed approach uses the hybrid approach using optimization with the supervised learning approach to train the system in such a manner that the system detect and mitigates the flooding attack to reduce the overhead consumption of the system.

Key Words: Packets, Attacks, Services, Nodes.

1. INTRODUCTION

A sensor network is an active research area with numerous workshops and conferences arranged each year. A Sensor Networks is a set of hundreds or thousands of micro sensor nodes that have capabilities of sensing, establishing wireless communication between each other and doing computational and processing operations. Most of the researchers found the collision problems between the packets which will degrade the performance and increase the energy consumption [1]. The work is done on the secure approach to reduce the energy consumption and computational costs. Depending on the network structure, different routing schemes fall into this category. Sensor network can be non-hierarchical or flat in the sense that every sensor has the same role and functionality. Therefore the connections between the nodes are set in short distance to establish the radio communication [2]. A lot of work is done using clustering approach in sensor networks for energy optimization and scaling of the network. Many network administrators found the problem of sudden increase in the energy consumption in packet transferring systems. As a result of which they uses clustering approach to decrease the energy consumption. A sensor network can be hierarchical or cluster-based hierarchical model, where the network is divided into clusters comprising of number of nodes. Cluster head, which is master node, within each respective cluster is responsible for routing the information to other cluster head. Another class of routing protocols is based on the location information of the sensor nodes either estimated on the basis of incoming signal strengths or obtained by small low-power GPS receivers or even by combination of the two previous methods. Location-based protocols use this information to reduce the latency and energy consumption of the sensor network.

Sensor Networks consists of spatially distributed autonomous sensor nodes to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. at different locations. Security is one of the main constraints in wireless sensor networks which are the big issue in real time scenarios. QOS optimization is the core issue in sensor networks because nodes are battery operated. Consequently many protocols have been

proposed in order to minimize the routing error of these nodes. As routing is one of the major tasks which is responsible in increasing lifetime of the network. The efficiency of sensor networks strongly depends on the routing protocol used. In this thesis, we will work on the performance of the energy minimization using hybridization of two algorithms used for the optimization. Sensor networks will be simulated using MATLAB. Several simulations will be conducted to analyze the performance of these protocols including the power consumption and overall network performance like energy consumption (Joules), packet delivery ratio, throughput (Mbps).

MANET deals with the decentralized wireless network systems. It deals with the mobile nodes which are free moving in free space path and out in the system. The sensor nodes are the devices which can be the mobile phone, personal digital assistance or personal computer which generally participates in the system and are mobile in nature. These sensor nodes can work as hosts at same times which are responsible in arbitrary topologies contingent on their connectivity with neighboring nodes in the system. These have the aptitude to arrange themselves and since of their self-configuration skill, they can be organized urgently deprived of the need of other structure. Internet Engineering Task Force has MANET environment that is dedicated for emerging IP routing procedures. Routing conventions is one of the stimulating and exciting research capacities for researchers. MANET security is one of the significant concerns for the basic purpose of network. Obtainability of network facilities, discretion and reliability of the information can be attained by promising that safety concerns which have been met. Ad-hoc networking often undergo from safety threats because of the its topographies like changing its network topology [17], absence of central observing and management, supportive algorithms and no defense process. These influences have altered the battle pitch condition for the MANETs alongside the safety issues. Ad-hoc networking work deprived of a centralized management where node interconnects with each other on mutual trust. This distinguishing deals MANETs more susceptible to be demoralized by an intruder from inside the system. Wireless associations also makes the MANETs extra susceptible to bouts which make it cooler for the aggressor to go exclusively in the network and get admittance to the communication. The mobile nodes existing within the choice of wireless link can hear and even contribute in the network systems.

The MANETs should have a protected technique for broadcasting and communication which is quite challenging and plays vital issue as here is increasing pressures of attack on the Network. To deliver secure communication and transmission an operator must appreciate different types of bouts and their belongings on the MANETs. Various types of threats like Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS) [12], that ad-hoc networks can suffer. MANETs are very crucial to these kinds of occurrences because broad casting is rely on shared trust among the nodes [4], there is no dominant point for system running, strongly altering topology and imperfect possessions.

In the previous couple of decades the world has turn into a worldwide town by prudence IT sector. Information Technology (IT) is developing step by step. Organizations have a tendency to utilize more difficult system situations. Regardless of the endeavors of system heads and IT merchants to secure the computing situations, the dangers posed to individual protection, organization security and different resources by attacks upon systems and PCs. The MANETs are unquestionably a piece of this revolution [1]. A MANET is an accumulation of wireless devices or hubs that impart by dispatching packets to each other or for another device/hub, without having any framework controlling information for routing. MANET hubs have boundless network and versatility to different hubs. Having a secured transmission and correspondence in MANET is a key issue because of the way that there are different sorts of attacks that the mobile system is interested in [2]. To secure correspondence in such systems, understanding the at risk security attacks to MANET is an extraordinary task and concern. MANETs experience the ill effects of a mixed bag of security attacks and dangers, for example, Denial of Service (DoS), flooding attack, mimic attack, wormhole attack, black hole attack, etc. [3].

In this thesis, energy optimization will be done using OLSR protocol to perform optimize routing in the mobile ad-hoc networks.

A network is a cluster connected with 3 or many notebook systems that are paired alongside to work collectively. It's really a telecommunication community that allows computers to change know-how. Within notebook sites, networked computing

devices go know-how for you to every distinct about know-how contacts [3].

Wi-Fi networking is a technology inside which in turn 3 or many computers converse collectively using very common community protocols even though without using cords[1]. The transmission takes place using the help of radio waves at actual physical stage.

It's but also known as Wi-Fi or WLAN. The IEEE standard pertaining to wireless network is 802.11.

Wireless networks can be classified into two types:

Infrastructure Network

Infrastructure-less Network

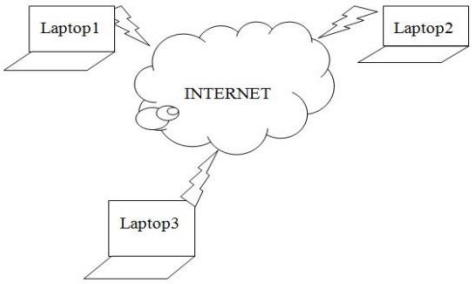

Figure1.1: Representation of Computer Network

The figure 1.1 shows the architecture in the wireless network form among the numerous laptop devices connected with each other.

A. Infrastructure Network

Within trade infrastructure primarily based network, communication takes place just between the Wi-Fi nodes and also the entry points. The particular communication won't right occur between the Wi-Fi nodes.

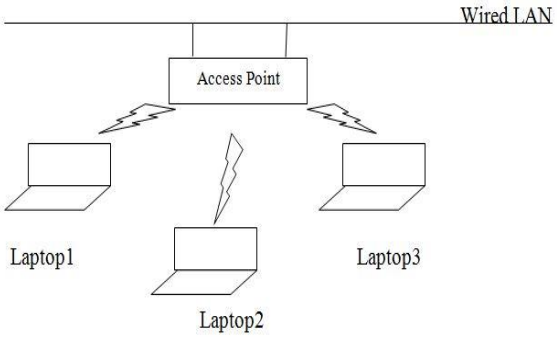

Figure 1.2: Infrastructure Network

B. Infrastructure-less Networks

The exacting infrastructure less network won't need any kind of commercial infrastructure to think. In this community, every node will converse right using distinct nodes. Therefore, in this community, not any entry purpose should be applied pertaining to dominating medium entry [4].

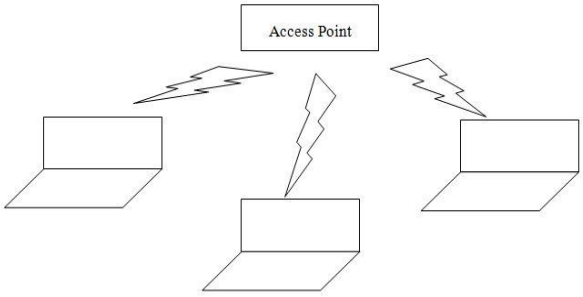

Figure 1.3: Infrastructure-less Network

Figure 1.3 shows the connection of the devices which doesn't need any infrastructure or which does not depend on any infrastructure. It can be portable

A mobile ad-hoc network is a network consisting of multiple wireless sensors, also called nodes, which cooperate in sensing some sort of physical or environmental conditions, such as temperature, sound, vibrations, light, movement etc. These networks can consist of everything from 10's of nodes for sparsely populated networks, up to 100's of thousands of nodes in densely populated networks. The individual sensor nodes are small and have limited energy, computational power and memory. This puts some restraints on the applications and protocols which are designed for use in such networks. Wireless sensor networks possess some unique characteristics which is listed below [4]:

-> Self-organizing

->Cooperating of sensor nodes

->Short range communication and multichip routing

->Limited energy, computational power and memory

->Dynamically changing topology

Table 1: Applications

Areas	Possible scenarios
Military Scenarios	Military communications and automated battle fields mainly based on MANET network.
Rescue	MANET helps in Disaster recovery, means additional of fixed infrastructure

Data networks	The exchange of data between mobile devices is also based on MANET.
Device operations	Wireless connections between various mobile devices are dependent on device networks.
Free internet connection	It also allows us to share the internet with other mobile devices.

The primary preferences of the Ad-hoc systems are depending on the subsequent:
1.It can be sub-urbanised construction that could be creating any place. There's no obligation pertaining to focal controller.
2.MANET works while not taking the help of previous systems.
3.It offers management in addition to having access to the marks on the location placement.
4.The idea illustrates deeply co-operative nature by means of as well as a lot of tools that are flexible.
The particular aggravations connected with MANET are while acquiring right after:
1. It can be limited assets.
2. It can be absence of backing administration.
3. Topology sequence frequently.
4. The exacting events that are exploiting being a section connected with wired systems can't be utilized being a section linked with impromptu systems.It's frightening to tell apart destructive centre thanks to development connected with topology.

Ad-Hoc network routing protocols are commonly divided into three main classes; Proactive, reactive and hybrid protocols as shown in figure [7].

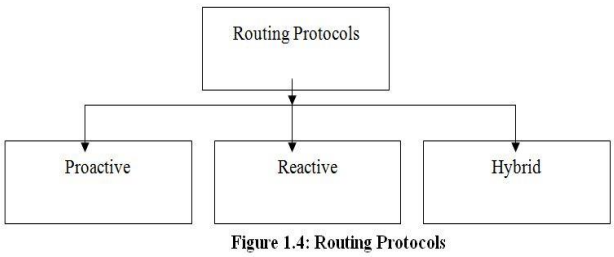

Figure 1.4: Routing Protocols

Figure 1.4 shows the different types of routing protocols which are used for the routing propose

Proactive Protocols: Proactive, or table-driven directing protocols. In proactive routing, every hub needs to keep up one or more tables to store directing data, and any adjustments in system topology should be reflected by spreading upgrades all through the system to keep up a steady system view. e.g.: Destination sequenced distance vector (DSDV). They endeavour to look after predictable, up and coming directing data of the entire system. It minimizes the delay in correspondence and permit hubs to rapidly figure out which hubs are available or reachable in the system.
Reactive Protocols: Reactive protocols is otherwise called on-demand directing protocol since they don't keep up directing data or directing action at the system hubs if there is no correspondence. In the event that a hub needs to send a bundle to another hub then this convention scans for the route in an on-interest way and sets up the connection so as to transmit and get the packet. E.g. Ad-hoc On-interest Distance Vector protocol (AODV) and Dynamic Source Routing (DSR).
Hybrid Protocols: They present a half breed model that consolidates receptive and proactive directing protocols. The Zone Routing Protocol (ZRP) is a half breed directing protocol that partitions the system into zones. ZRP gives a various levelled structural engineering where every hub needs to keep up extra topological data obliging additional memory. When considering route creation process, routing protocols can be classified in three main categories: proactive, reactive and hybrid, as described below.

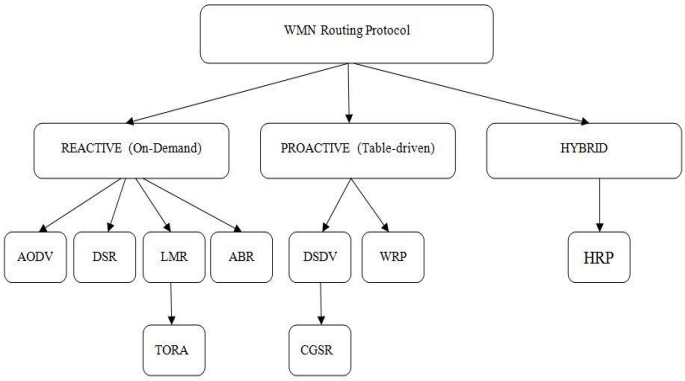

Figure 1.5 (Different Routing Protocols)

Figure 1.5 shows the different routing protocols with their families that which category belongs to which family member in the routing protocol family:

1.Destination-Sequenced Distance-Vector (DSDV)

The Destination-Sequenced Distance-Vector (DSDV) [14] Routing Algorithm is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements. Every mobile station maintains a routing table that lists all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination node. The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbours. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So, the update is both time-driven and event-driven.

2.Wireless Routing Protocol (WRP)

The Wireless Routing Protocol (WRP) [41] is a table-based distance-vector routing protocol. Each node in the network maintains a Distance table, a Routing table, a Link-Cost table and a Message Retransmission list. The Distance table of a node x contains the distance of each destination node y via each neighbour z of x.

3.Global State Routing (GSR)

Global State Routing (GSR) [14] is similar to DSDV. It takes the idea of link state routing but improves it by avoiding flooding of routing messages.

In this algorithm, each node maintains a Neighbour list, a Topology table, a Next Hop table and a Distance table. Neighbour list of a node contains the list of its neighbours (here all nodes that can be heard by a node are assumed to be its neighbours.). For each destination node, the Topology table contains the link state information as reported by the destination and the timestamp of the information. For each destination, the Next Hop table contains the next hop to which the packets for this destination must be forwarded. The Distance table contains the shortest distance to each destination node.

4.Hierarchical State Routing (HSR)

The characteristic feature of Hierarchical State Routing (HSR) is multilevel clustering and logical partitioning of mobile nodes. The network is partitioned into clusters and a cluster-head elected as in a cluster-based algorithm. In HSR, the cluster-heads again organize themselves into clusters and so on. The nodes of a physical cluster broadcast their link information to each other. The cluster-head summarizes its cluster's information and sends it to neighbouring cluster-heads via gateway.

5.Power-Efficient Gathering in Sensor Information Systems (PEGASIS)

PEGASIS is a redirecting method when a chain primarily based method is usually followed. This method employs some sort of greedy approach beginning from the actual furthermost node and each of the sensor nodes form some sort of string just like composition. It functions for the process that many node will probably transfer in order to and acquire via it's in close proximity neighborhood nodes. There's a leading light in the string which is in charge of transmitting in the collective facts towards sink node. Nodes take transforms being the best in the network which smoothly allocates the energy load between the nodes. This also do energy sharing and large energy proficiency contributes to the actual extension in the network life span. It tries to cut back the actual delay the fact acquires on the way towards bottom station [15]. Fig. shows the actual on-line of sensor nodes within PEGASIS method.

A) Optimized Link State Routing Protocol (OLSR)

The Optimized Link State Routing Protocol(OLSR) is an IP routing protocol optimized for mobile ad hoc networks, which can also be used on other wireless ad hoc networks. OLSR is a proactive link-state routing protocol, which uses hello and topology control (TC) messages to discover and then disseminate link state information throughout the mobile ad hoc network. Individual nodes use this topology information to compute next hop

destinations for all nodes in the network using shortest hop forwarding paths [17].

In correlation with table-based routing protocols, in this class of protocols, not every single updated route is put away on every hub; rather, the routes will be developed at whatever point they are required. At the point when a source hub needs to send one message to a destination, it will request the route discovery mechanisms to find a route to the destination, Route Reply (RREQ). A route stays legitimate until the destination is accessible. RREP component sends, backward, the route to source hub. CBRP (Cluster Based Routing Protocol), AODV, DSR, TORA (Temporally Ordered routing protocol) & ABR (Area Border Router) are a few illustrations of need-based protocols.

Three types of OLSR messages:

a) Hello

This control message is transmitted for sensing the neighbour and for Multi Point Distribution Relays (MPR) calculation.

b) TC

Topology Control (TC) these are link state signaling that is performed by OLSR. MPRs are used to optimize theses messaging.

c) MID

Multiple Interface Declaration (MID) messages contain the list of all IP addresses used by any node in the network. All the nodes running OLSR transmit these messages on more than one interface.

- OLSR does not need central administrative system to handle its routing process.
- The link is reliable for the control messages, since the messages are sent periodically and the delivery does not have to be sequential.
- OLSR is suitable for high density networks.
- It does not allow long delays in the transmission of packets

d) RBDRP

There are large number of packet forwarding methods like reward based, behavioural based, reputation based. But Reward based is best one. While encouraging forwarding, a balance must be maintained between forwarding and self-transmissions. Reward-based systems reward a node with credits that forwards for other nodes, so it can use the credits to pay other nodes for its multi-hop self-transmission. One implementation is the use of a counter maintained at each node, where counter is a virtual currency. When a node needs to transmit a self-generated data packet, its counter will be decremented. But the counter can be incremented again when this node forwards data packets for other nodes. When the counter goes to zero, which means a node has transmitted more self-generated packets than forwarded packets, it will not be allowed to transmit any more self-generated packets.

Reward function can be defined as:

If pair {S, D} exists in the routing table with a source $-$ sequence $-$ number of sqn2,

If (Ri $>$ 0 and sqn1 $=$ sqn2) or (sqn1 $>$ sqn2),

X updates the routing table.

B.Moth Flame optimization algorithm

Moth Flame Algorithm basically utilizes the accompanying three admired principles:

- Moth Flame is unisex. The dragging of one firefly to another firefly hardly matters on the sex of firefly.
- The appeal is relative to the splendour, and they both lessening as their separation increments. Consequently for any two powerful moths, the less lively single will exchange near the brighter one. In the event that here is never a brighter firefly than a specific moth, they change arbitrarily.
- They move randomly if there are no fireflies brighter than the given one.

Since a moths engaging quality is relative to the light power shown by adjacent moths, it can now characterize the variety of allure β with the separation r by

$B = \beta 0\ e^{-\gamma r2}$

Where β0 is the allure at r = 0.

1.2 UNCERTAINTY IN MANET

In recent years [8] the concern over the security of computer networks has been widely discussed and popularized. The discussion has, however, typically involved only static and wired networking while the mobile or ad-hoc networking issues have not been handled extensively. The emergence of such new networking approaches sets new challenges even for the fundamentals of routing since the mobile ad-hoc networks (MANET) are significantly different from the wired networks. Moreover, the traditional routing protocols of the Internet have been designed for routing the traffic between wired hosts connected to a static backbone; thus, they cannot be applied to adhoc networks because the basic idea of such networks is mobility with dynamic topology.

Black hole problem in MANETS is a serious security problem to be solved. In this problem, a malicious

node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In flooding based protocol, if the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. This malicious node then can choose whether to drop the packets to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack. Mobile Ad-Hoc Networks are autonomous and [8] decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self-configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc.

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

In flooding, a malicious node uses its routing protocol to send the unnecessary requests and packets to the centralized unit to effect the network deeply. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address.

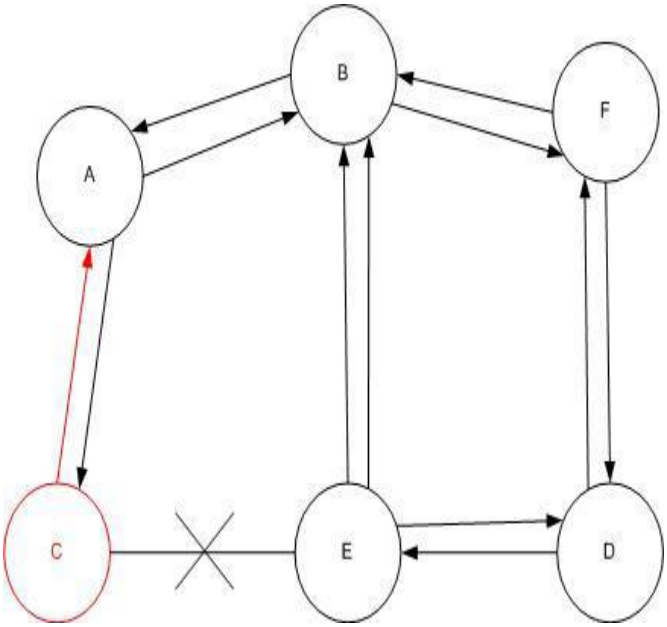

Figure 1.3 Uncertainty Process

2. LITERATURE SURVEY

Farhad Akhoundi, Mohammad Vahid Jamali, Navid Bani Hassan, Hamzeh Beyranvand, Amir Minoofar et al. [1] proposed network which is used as substructure of centralized, dispersed and relay-assisted sensor networks for real-time monitoring. Lastly, probable plan challenges like cell edge

coverage, obstruction evasion, power regulator and network volume are addressed.

Abdul Wahid and Dongkyun Kim et al.[2] proposed energy resourceful routing procedure, named EEDBR which is popularly known as energy-efficient depth-based routing protocol. EEDBR exploits the complexity of sensor nodes for advancing data packets. Also, the residual liveliness of sensors is also occupied into explanation in order to recover the network lifetime.

Salvador Climent, Antonio Sanchez, Juan Vicente Capella, Nirvana Meratniaand Juan Jose Serrano et al.[3] proposed security threads and reviews the currently future studies. Present envisioned places for further developments in sensor networks research series from efficient, low-power procedures and variations to intelligent, energy-aware overpowering and medium access controller manners.

Yuh-Shyan Chen, Yun-Wei Lin and Sing-Ling Lee et al.[4] proposed new mobicast procedure is obtainable in their work to successfully distribute mobicast communications to all means of transportation in ZOR via a singular geographic zone, named as zone of forwarding procedure (ZOF). The main influence of this work is to progress a new mobicast routing procedure to energetically estimate the precise ZOF to positively disseminate mobicast communications to all nodes in ZOR.

Jaydip M. Kavar,Dr.K.H Wandra et al. [5] deliberate the internal construction of sensor networks, they have discussed the fiction of sensor network, dissimilar architectures for 2-D and 3-D sensor networks are deliberated, They have also conversed the submission and main difficulty or problem in sensor network.

Ujala Zaffer Raina, Himali Sarangal, Neetika Soni et al, [6] have considered and reviewed the developing technology of Sensor Networks. The challenges that encounters in emerging them and the submissions. They have determined with a future view of their present work. Sensor networks has appeared as one of the greatest hot topics of investigation in wireless skills because of its practicality in the stimulating conditions in which previous the data gathering was very tough.

Monowar H. Bhuyan, D. K. Bhattacharyya, J. K. Kalita et al. [8] (2014) presented an approach in which information theory is used and abnormal network behaviours. Based on the mutual information between network features and the types of network intrusions, a small number of network features were closely identified with network attacks. Then a linear structure rule is derived using the selected features. The use of mutual information reduced the complexity, and the single resulting linear rule made the intrusion detection efficient in real-time environment. However, the author approach considered only discrete features.

Kalsoom Shabana, Nigar Fida, Fazlullah Khan, Syed Roohullah Jan, Mujeeb Ur Rehman [9] (2016) presented such issues to detect network anomalous. The detection rates might be increased due to quantitative features inclusion. Parameters and evolution processes are discussed in details. They have introduced issues which used evolution theory to information evolution in order to filter the traffic data and thus reduce the complexity.

Daniel-Ioan Curiac (2016) [11] proposed a methodology to detect network anomalies using Directional antennas. They provide solutions to decrease the security risks to use directional projections instead of omnidirectional ones or in conjunction with them.

Gorine, habib et.al. [12] (2016) have security issues and experiments facing investigations in wireless sensor networks and measures to solve them. The transmission nature of wireless communication creates Wireless Sensor Networks disposed to numerous attacks.

Oh, Y. J., & Lee, K. W. et al. [14] (2017) the authors proposed a neural network based security in processors, providing Internet services. Most controlled neural net constructions required reskilling in order to increase analysis capability due to dynamic changes in the data, but unconfirmed net offers amplified level of flexibility to neural nets and dynamically improve their analysis proficiency. Generally network systems in unsubstantiated which used self-organizing maps neural nets and only a few schemes used additional categories of unsupervised neural networks.

Sagar R. Deshmukh, Dr. P. N. Chatur et al. proposes a DSR secure direction-finding to notice black hole attack. The planned solution, assigns a validity charge with RREP. The rationality value is patterned by the first transitional hop along the road reply and guarantees that nearby is no black hole bout along the track.

Arash Tayebi, Setevan Berber, Akshya Swain et al. [16] proposed investigation of the possible network threats which are essential for scientists or various researchers in developing strong security preferences. In their study, the author proposed overview of numerous threats of sensor networks and also they have done a critical study of the traditional research performance. Based on their analysis, they suggest developing efficient secure procedures which is to be known as cross-layer threats, which associates and shows the merits of various attacks based on numerous layers.

Muhammad Raisuddin Ahmed et al. [17] examines internal security matters in wireless sensor networks and advises relevant explanations. They have worked on the growth of multi stage apparatuses to secure sensor networks from interior attacks. The chief contributions of their research is to stop internal bouts

Vladimir V. Shakhov et al. [18] discussed various critical threats of wireless sensor networks which is a deprived of sensor battery. It deals to sensor susceptibility for battery draining threats. Quick exhaustion of battery influence is not only described by interruptions but also by a breakdown of networks procedures. In their research they have investigated the Daniel of service attacks and evaluate the performance of the network

Hector Kaschel, Jose Mardones, Gustavo Quezada et al. [19] analyse security necessities of sensor networks, the significant attacks, and also the features and eventually they have reviewed some procedures which are currently implemented in sensor systems, and recognizes the conceivable types of safety threats that can disturb the coatings of the OSI model layers

Mulla [35] proposed an associate economic Analysis of light-weight Sybil Attack Recognition theme in Mobile Ad hoc Networks. Author inspected this methodology using network simulator named as NS2. The sensible examination of this approach is finished by considering 3 network conditions like traditional network behavior, presence of Sybil wrongdoer nodes in network and eventually planned approach to discover such Sybil intruders in the network systems. The performance evaluation is ended among these 3 varieties of network conditions with intention of accomplishing performance of prearranged procedure is analogous to traditional condition of the network. From results it's clear with RSS even with presence of Sybil attackers, the investigated methodology works with efficiency and doesn't results into any data loss. The sole limitation of this methodology is that high end to end delay as compared to traditional network condition.

Kasiran and Mohamad [36] analyzed the turnout of AODV below hollow and Sybil Attack. During this paper author assess the turnout AODV performance with the existence of hollow and Sybil attack. The consequences have revealed that there's distinction performance in turnout once there's associate attack. The performance analysis shows that the turnout just in case of presence of hollow attack and Sybil attack is decrease than that within the absence of such a node.

Patidar et al. [37] changed the routing of AODV process for interference against Black and heat hole attack. The paper proposes protocols which can defend important networks consist of the black hole and hollow occurrences and to boost the stability. This paper deals with the associate intrusion sighting system supported the thought of specification rely detection approach to distinguish and prevent black hole attacks. This paper additionally deals with the counting of hopes to detect the hollow attacks on routes in impromptu networks. The projected protocol doesn't need any position info, interval synchronization to sight hollow attacks. in step with simulation, the projected techniques work with superior evaluations as delivery ratios and turnout will increase but, average end-to-end delay additionally will increase. Within the analyzed situation, it's found that the changed AODV and IDS-AODV has superior performance than AODV.

Alvisi et al. [38] analyzed the SoK: The Evolution of Sybil Defence via Social Network. In general the social network operatives are in a location to use mechanism learning systems, operator profiling, and intensive care of worker motion to gain additional information that can assist them and filter Sybil doses which are not well–suited for recognition using practices grounded on random walks, communal detection, and their grouping. Still, as invaders increase in cleverness, entitlements of silver ammunition should be encountered with healthy situations. As the weaponries race among attackers and protectors continues, it will be gradually imperative that new defense machineries clearly state-run the kind of occurrence they goal to with stand, a countryside that too habitual is blurred.

Liu et al. [39] defined a scheme to use signal designs to perceive Sybil attacks in uncluttered ad hoc and delay-tolerant systems without necessitating belief in any other bulge or specialty. We use the characteristic difficulty of forecasting RSSIs to discrete factual and false RSSI explanations described by one-hop nationals. Aggressors using motion to downfall the signal reproduction procedure are distinguished by demanding low-latency retransmissions through the same location. The test was executed on HTC smartphones and verified with human contributors in three surroundings. It abolishes 99.6–100 out of a hundred of Sybil characteristics in office atmospheres, 91 percentages in a crowded high gesture cafeteria, and 96 out of a hundred in a high-motion uncluttered outdoor situation. It accepts 88–97 percent of compatible characteristics in the office surroundings, 87 out of a hundred in the cafeteria, and 61 out of a hundred in the outdoor

atmosphere. The vast mainstream of rejected compatible identities was eradicated due to motion.
Feng et al. [40] proposed a process for defending against multi-source Sybil bouts in VANET. In this weekly, author recommend an event based standing system, in which dynamic standing and trusted charge for each occurrence are employed to conquer the supper of false letters. The structure can detect Sybil outbreak with fabricated personalities and stolen individualities in the procedure of communication which also defends in contradiction of the conspired Sybil bout since each happening has a unique standing value and important value.
Biswas et al. [41] had projected hollow detections and interference Technique in Edouard Manet victimization changed AODV Protocol. Author proposes associate rule to sight wormholes with none special hardware. Their research is associate improvement over antecedent given WAP in a very method that WAP deals with the false detection wherever as WADP is not able to detect the false things once exposed hollow attack area unit launched because it involves detection of wicked nodes through reliably take a look at and supplementary confirmation of resonating presence by calculative interruption per hop of unprotected bouts and by neighbour node reflection in case of concealed attacks. Their instrument is compulsory supported the different AODV protocol.
Ji et al. [42] projected associate rule for defensive against hollow Attacks in Wireless Network writing Systems. Author projected a Distributed detection rule against hollow in wireless Network writing systems. It is completely distributed for the nodes within the network, eliminating the limitation of tightly synchronised clock. It is efficient and therefore it fits for wireless detector network. Author utilizes the digital signatures to make sure each report is plain and can't be solid by any attackers. The simulations have shown that the projected rule will sight the malicious nodes collaborating in hollow attack with high winning rate and therefore the rule is efficient in terms of computation and communication overhead.
Dutta and Biswas [43] analysed impact of heat hole attack on OLSR routing protocol. A modified version of hollow attack is developed during this paper, referred to as camouflaging hollow attack, and a corresponding specification primarily based IDS is intended to sight and forestall this attack. Camouflaging hollow attack maintains a non-public tunnel between 2 nodes and typically assailant nodes additionally drop some packets like region attack. The attack is launched, still there's no delay and it looks to be no hollow attack.
Han et al. [44] had projected passive and period of time theme mutely observes the variations in topology to infer the hollow existence. Our approach depends entirely on network routing info and doesn't necessitate specialised hardware or poses rigorous assumptions on network options. Author assess the network scales comprising of one hundred to five hundred nodes show that P-worm achieves superior performance and pertinence on false negative, time delay and quantifiability.
Lee et al. [45] studied the Passivity approach for mitigations of the malicious attacks. Author progress this outline for each frequency band hollow attacks likewise as complicated, hereto-unreported hollow occurrences containing of discretional combinations of malicious nodes or wormholes. By group action existing justification methods into their framework, they are having a tendency to analyze the turnout, delay, and properties for stabilize general system. The simulation consequences demonstrate the trade-off among the effectiveness of the network defence and therefore the upsurge in delay. Above all, we have a tendency to initiate that hollow attack causes massive disturbances within the corporal system by selection dropping envelopes, and therefore the parameters secure packets will be chosen to cut back flow distribution to the hollow.
Patel et al. [46] had projected rule to defensive against hollow Attack in MANET. Author projected approach based mostly on the Hash based Compression operate that is truly victimization any secure hash operate to calculate a price of hash field for route request packet. The projected approach appearance terribly promising compared to different potential explanations in literature study. All the reproductions are performed in NS2 machine victimization AODV routing protocol.

3. PROPOSED WORK

3.1. Existing Work

Sensor Networks consists of spatially distributed autonomous sensor nodes to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. at different locations. Energy is one of the main constraints in wireless sensor networks which are the big issue in real time scenarios. QOS optimization is the core issue in sensor networks because nodes are battery operated. Consequently many protocols have been proposed in order to minimize the routing error of these nodes. As routing is one of the major tasks which is responsible in increasing lifetime of the network. The efficiency of sensor networks strongly depends on the routing protocol used.

Various researches are done on the routing using security analysis in mobile ad-hoc networks. These networks are having high impact on sending information at larger distances. These are infra-structure less systems which are used for the monitoring of the systems. The sensor network is an active research area with numerous workshops and conferences arranged each year. A Sensor Networks is a set of hundreds or thousands of micro sensor nodes that have capabilities of sensing, establishing wireless communication between each other and doing computational and processing operations. Sensor networks have a wide variety of applications and systems with vastly varying requirements and characteristics. The sensor networks can be used in Military environment, Disaster management, Habitat monitoring, Medical and health care, Industrial fields, Home networks, detecting chemical, Biological, radiological, nuclear, and explosive material etc. So this thesis put light on such efficient protocols which are used for the optimization of sensor networks.

The existing works deals with the conservation of energy on the various security processes in which the system is having less energy conservation in the terms of conservation of energy.

3.2 Methodology

The proposed work deals with the optimization algorithm process using moth flame optimization and back propagation neural network which is having less uncertainties and having high packet deliveries and throughputs.

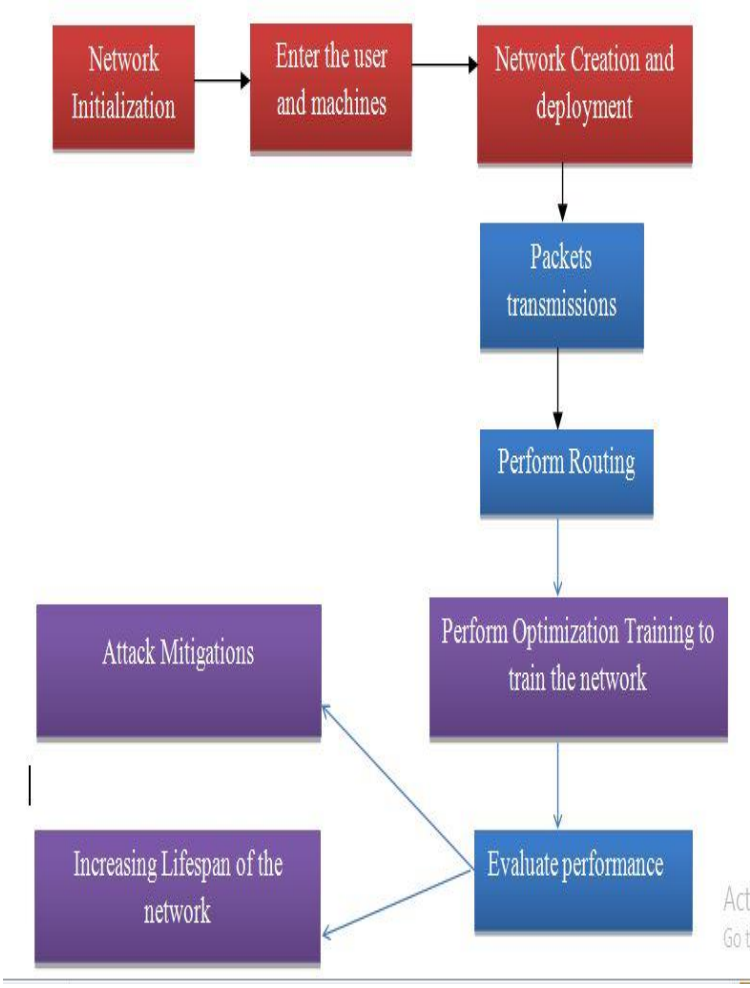

Figure 3.1: Proposed Flow Diagram

4. IMPLEMENTATION AND RESULT DISCUSSIONS

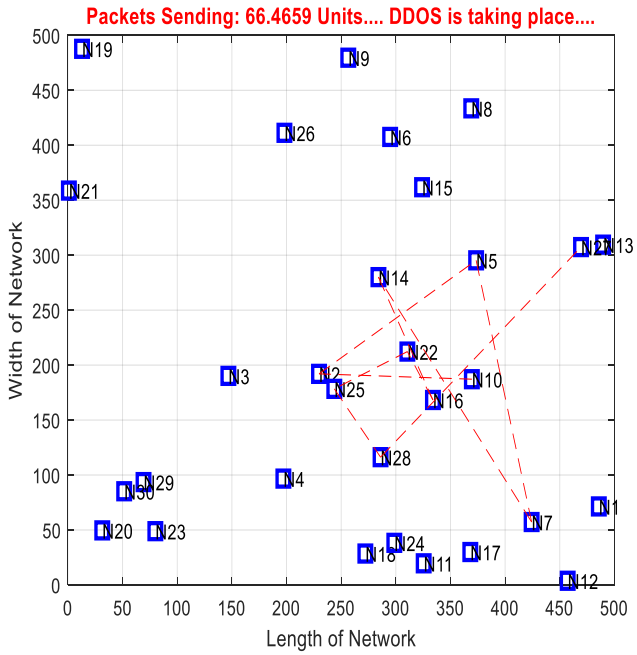

Figure 4.1 Network Creation

The figure 4.1 shows the network creation in which nodes are deployed the communication is done as per the network nodes. The Nodes are plotted blue in color and shows that the packet sending as per the DDOS attack occurred during transmissions. The blue line is showing the link among the nodes which are transmitting the packets in the sensor networks.

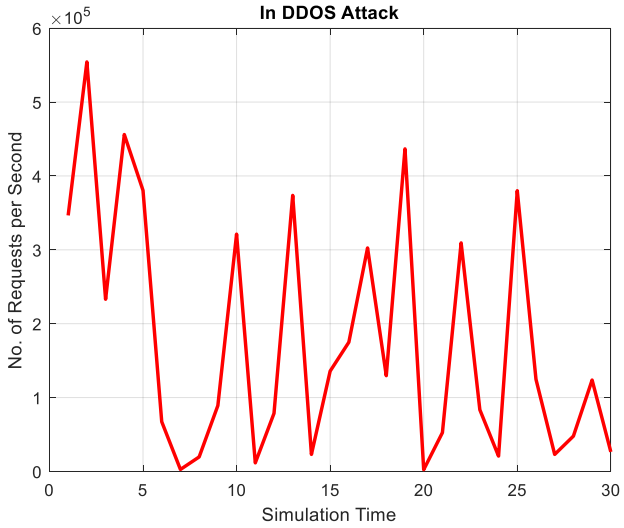

Figure 4.2 No. of requests/second

The figure 4.2 shows the request increases on the networks due to the DDOS effect which shows that the loading on the nodes are increasing at the certain limit where the congestion among the networks are increasing which can increase the overhead consumption and failures among the nodes.

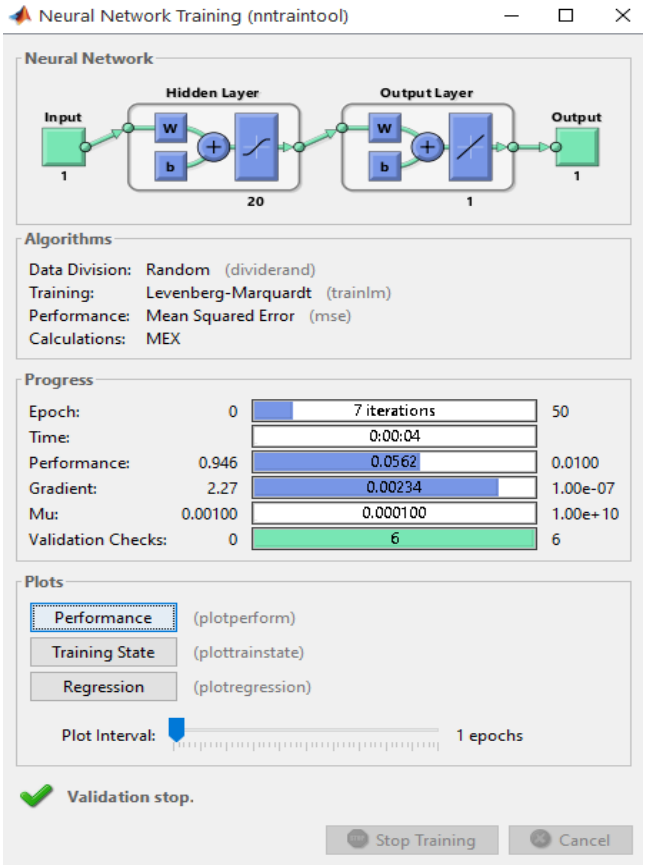

Figure 4.3 Network Training

The figure 4.3 shows the training of the network and shows that the proposed approach is able to achieve high performance in terms of efficient training to reduce the error rates in the performance of the system in a back propagation scenario.

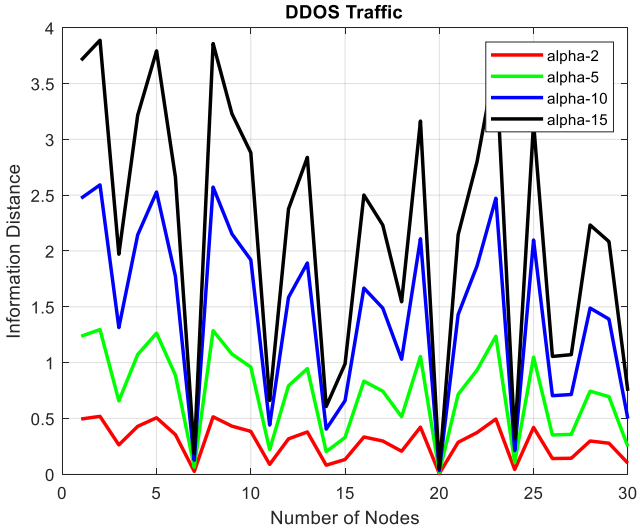

Figure 4.4 DDOS Traffic classifications

The figure 4.4 shows the DDOS traffic classifications which show that the proposed machine learning approach is able to achieve the traffic classifications in terms of DDOS traffic to mitigate and regulations among transmissions which is one of the significant approach for the efficient network lifetime.

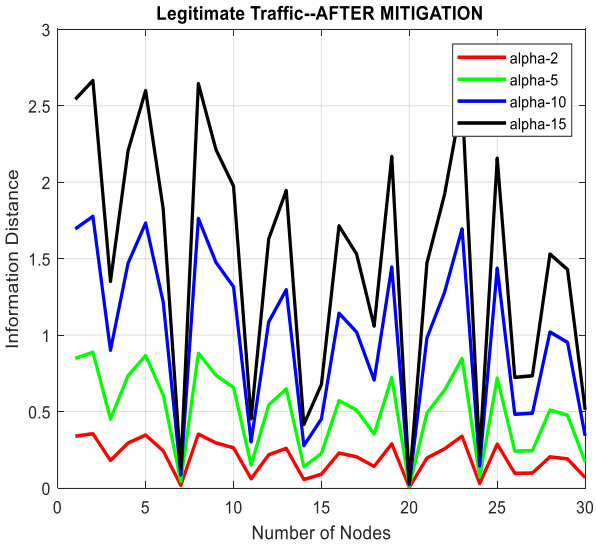

Figure 4.5 Legitimate traffic

The figure 4.5 shows the legitimate traffic which is one of the mitigation effects of the DDOS effect where the base station can distinguish that the traffic coming among the nodes are DDOS traffic or legitimate traffic. The traffic must be distinguished for the proper functioning of the network so that the network lifetime must be increased without any failures.

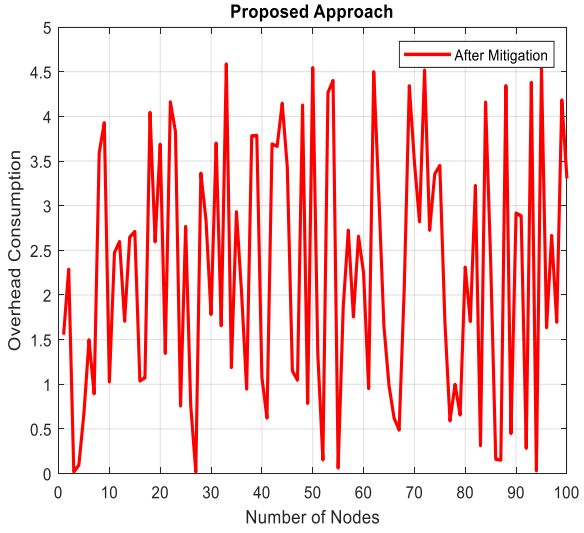

Figure 4.6 Overhead Consumption

The figure 4.6 shows the overhead consumption which must be reduced for the efficient network lifetime. The overhead increases the load on the network nodes and is responsible in dropping the packets which will degraded the network performance for high evaluations of the packet deliveries at the sink node or the base station.

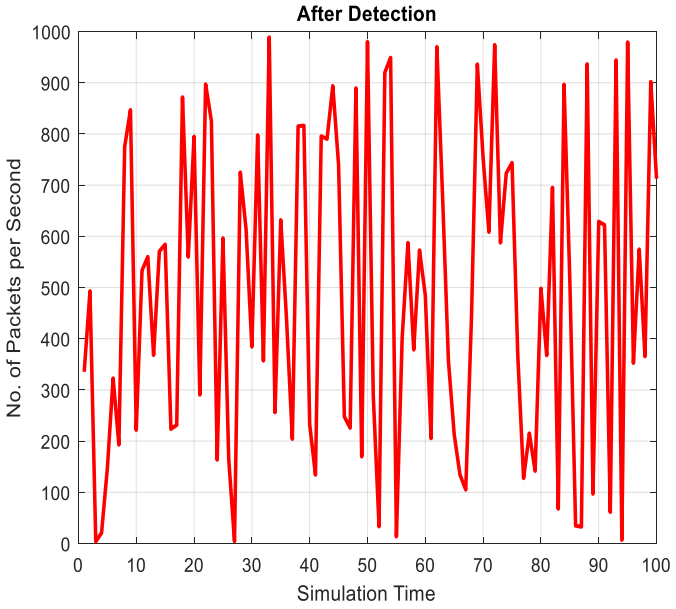

Figure 4.7 No. of packets/Sec

The figure 4.7 shows the number of packets among the network per second which shows the high efficiency of the network to receive the packets in an efficient way with the efficient balancing of the load. This shows that proposed approach is able to achieve high performance of the mitigation of the attack in the network which will further reduce the overhead consumptions.

4.1 SIMULATION TOOLS

Table 4.1: Tools used

Computer	Core 2 Duo or higher
RAM	3 GB
Platform	Windows 7
Other hardware	Keyboard, mouse
Software	Matlab 2016

5. CONCLUSION AND FUTURE SCOPE

In the proposed approach the work is done to optimize the network using machine learning back propagation neural network in hybridization of the optimization to achieve the performance evaluations in terms of mitigation effect. Because of the limited resources of the nodes, it is necessary for the nodes to collaborate with each other. Numerous nodes may be tasked with detecting the same singularity these nodes may collaborate in a collection where node is tasked with condensing the sensor consequence from all the other nodes in the collection and shows that the system is having less losses and is able to tackle the problems of uncertainties like energy failures, attacking in the network which will increase the load in the network which shows that the system is having high throughput and packet deliveries with less number of error rates. So eventually the proposed approach is able to achieve mitigation scenario of the DDOS attack to have high network performance.

The future work can be the optimization with the hybrid approach of the other optimization algorithms to reduce the uncertainties to achieve less error rate probabilities.

REFERENCES

[1] Akhoundi, F., Jamali, M. V., Hassan, N. B., Beyranvand, H., Minoofar, A., & Salehi, J. A. (2016). Cellular underwater wireless optical CDMA network: Potentials and challenges. IEEE Access, 4, 4254-4268.

[2] Wahid, A., & Kim, D. (2012). An energy efficient localization-free routing protocol for underwater wireless sensor networks. International journal of distributed sensor networks, 8(4), 307246.

[3] Climent, S., Sanchez, A., Capella, J. V., Meratnia, N., & Serrano, J. J. (2014). Underwater acoustic wireless sensor networks: advances and future trends in physical, MAC and routing layers. Sensors, 14(1), 795-833.

[4] Chen, Y. S., Lin, Y. W., & Lee, S. L. (2010). A mobicast routing protocol in vehicular ad-hoc networks. Mobile Networks and Applications, 15(1), 20-35.

[5] Kavar, J. M., & Wandra, K. H. (2012). Survey paper on Underwater Wireless Sensor Network.

[6] Raina, U. Z., Sarangal, H., & Soni, N. (2016). A Review on Underwater Wireless Sensor Networks. Wireless Communication, 8(4), 119-123.

[7] Cheng, E., Lin, X., Chen, S., & Yuan, F. (2016). A TDoA Localization Scheme for Underwater Sensor Networks with Use of Multilinear Chirp Signals. Mobile Information Systems, 2016.

[8] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014, August). Information metrics for low-rate DDoS attack detection: A comparative evaluation. In Contemporary Computing (IC3), 2014 Seventh International Conference on (pp. 80-84). IEEE.

[9] Anwar, R. W., Bakhtiari, M., Zainal, A., Abdullah, A. H., Qureshi, K. N., Computing, F., & Bahru, J. (2014). Security issues and attacks in wireless sensor network. World Applied Sciences Journal, 30(10), 1224-1227.

[10] Bridges, S. M., & Vaughn, R. B. (2000, June). Intrusion detection via fuzzy data mining. In 12th Annual Canadian Information Technology Security Symposium (pp. 109-122)

[11] Curiac, D. I. (2016). Wireless sensor network security enhancement using directional antennas: State of the art and research challenges. Sensors, 16(4), 488.

[12] Gorine, H., & Elmezughi, M. R. (2016). Security threats on wireless sensor network protocols. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 10(8), 1523-1526.

[13] Singh, T., Singh, J., & Sharma, S. (2017). Energy efficient secured routing protocol for MANETs. Wireless Networks, 23(4), 1001-1009.

[14] Oh, Y. J., & Lee, K. W. (2017). Energy-efficient and reliable routing protocol for dynamic-property-based clustering mobile ad hoc networks. International Journal of Distributed Sensor Networks, 13(1), 1550147716683604.

[15] Deshmukh, S. R., & Chatur, P. N. (2016, March). Secure routing to avoid black hole affected routes in MANET. In Colossal Data Analysis and Networking (CDAN), Symposium on (pp. 1-4). IEEE.

[16] Tayebi, A., Berber, S. M., & Swain, A. (2015). Wireless Sensor Network Attacks: An Overview and Critical Analysis with Detailed Investigation on Jamming Attack Effects. In Sensing Technology: Current Status and Future Trends III (pp. 201-221). Springer International Publishing

[17] Huang, X., Ahmed, M. R., Sharma, D., & Cui, H. (2013, April). Protecting wireless sensor networks from internal attacks based on uncertain decisions.

In Wireless Communications and Networking Conference (WCNC), 2013 IEEE (pp. 1854-1859). IEEE.

[18] Shakhov, V. V. (2013, June). Protecting wireless sensor networks from energy exhausting attacks. In International Conference on Computational Science and Its Applications (pp. 184-193). Springer, Berlin, Heidelberg

[19] Kaschel, H., Mardones, J., & Quezada, G. (2013). Safety in Wireless Sensor Networks: Types of Attacks and Solutions. Studies in Informatics and Control, 22(3), 323-329.

[1] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Mesh Networks," in the Proceedings of the First Workshop on Mesh Networks and Applications (MANETA), Atlanta, GA, October 2002.

[2] F. Ye, A. Chen, S. Liu, L. Zhang, "A scalable solution to minimum cost forwarding in large mesh networks", Proceedings of the tenth International Conference on Computer Communications and Networks (ICCCN), pp. 304-309, 2001.

[3] N. Sadagopan et al., The ACQUIRE mechanism for efficient querying in mesh networks, in the Proceedings of the First International Workshop on Mesh Network Protocol and Applications, Anchorage, Alasa, May 2003.

[4] V. Rodoplu and T. H. Meng, "Minimum Energy Mobile Wireless Networks", IEEE Journal Selected Areas in Communications, vol. 17, no. 8, Aug. 1999, pp. 133344.

[5] Shurman,M.M.; Al-Mistarihi, M.F. ; Mohammad, A.N. ; Darabkh, K.A. and Ababnah, A.A.," Hierarchical clustering using genetic algorithm in wireless mesh networks", Published in : Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention, Print ISBN: 978-953-233-076-2,May 2013.

[6] Gao Yang,Zhuang Yi , Ni Tianquan, Yin Keke and Xue Tongtong," An improved genetic algorithm for wireless mesh networks localization" Bio-Inspired Computing: Theories and Applications (BIC-TA), 2010 IEEE Fifth International Conference, Sept. 2010.

[7] Sajid Hussain, Abdul W. Matin and Obidul Islam, "Genetic Algorithm for Energy Efficient Clusters in Wireless Mesh Networks", IEEE.

[8] Bojan, S. ; Inst. Mihajlo Pupin, Univ. of Belgrade, Belgrade, Serbia; Nikola, Z., "Genetic algorithm as energy optimization method in MANET ", IEEE, pp.97-100, 2013.

[9] Ali Norouzi and A. Halim Zaim, "Genetic Algorithm Application in Optimization of Wireless Mesh Networks", Hindwai, 2013.

[10] K. Akkaya and M. Younis, "An Energy-Aware QoS Routing Protocol for Wireless Mesh Networks," in the Proceedings of the IEEE Workshop on Mobile and Wireless Networks (MWN 2003), Providence, Rhode Island, May 2003.

[11] Meenu and Vandana M.Tech, M., C. S. E. Deptt, and Haryana Sonepat. "Modified PEGASIS in MANET to increase Network Lifetime.", 2012.

[12] Rana, Hetal, S. Vhatkar, and M. Atique. "Comparative Study of PEGASIS Protocols in Wireless Mesh Network.", 2015.

[13] S. Rani, T. Gulati" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 11, November 2012.

[14] B. Singh et al Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 3(Version 1), March 2014.

[15] P. Kumar, M.P.Singh and U.S.Triar" A Review of Routing Protocols in Wireless Mesh Network" International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 4, June - 2012 ISSN: 2278-0181

[16] Malathi, L., and R. K. Gnanamurthy. "Cluster Based Hierarchical Routing Protocol for MANET with Energy Efficiency.", 2012.

[17] Weiwei Fang, Zhen Liu and Feng Liu" Weiwei Fang, Zhen Liu and Feng Liu A Cross-Layer Protocol For Reliable And Efficient Communication In Wireless Mesh Networks International Journal of Innovative Computing, Information and Control ICIC International c 2012 ISSN 1349-4198 Volume 8, Number 10(B), October 2012

[18] Martin Engineer" Energy-efficient communication in Wireless Mesh Networks Seminar SN SS2012 doi: 10.2313/NET-2012-08-2_04 Network Architectures and Services, August 2012

[19] "1Chellaprabha, B. and 2S. Chenthur Pandian" A Multipath Energy Efficient Congestion Control Scheme for Wireless Mesh Network Journal of Computer Science 8 (6): 943-950, 2012 ISSN 1549-3636 © 2012 Science Publications.

[20] Selcuk Okdem and Dervis Karaboga: Routing in Wireless Mesh Networks Using an Ant Colony Optimization (ACO) Router Chip: In Meshs 2009.

[21] Shio Kumar Singh, M P Singh, and D K Singh: Energy Efficient Homogenous Clustering Algorithm for Wireless Mesh Networks: International Journal of Wireless & Mobile Networks (IJWMN), Vol.2, No.3, August 2010.

[22] Y. Zhang, L. D. Kuhn, and M. P. J. Fromherz, "Improvements on Ant Routing for Mesh Networks," M. Dorigo et al. (Eds.): ANTS 2004, Springer-Verlag

Berlin Heidelberg 2004, vol. LNCS 3172, pp. 154-165, 2004.

[23] Tiago Camilo, Carlos Carreto, Jorge Sá Silva, Fernando Boavida: An Energy-Efficient Ant-Based Routing Algorithm for Wireless Mesh Networks.

[24] Rabiner, W.; Kulik, J.; Balakrishnan, H. Adaptive Protocols for Information Dissemination in Wireless Mesh Networks. In Proceedings of the Fifth Annual International Conference on Mobile Computing and Networking (MOBICOM), Seattle, WA, USA, August, 1999; pp. 174–185.

[25] Heinzelman, W.B.; Chandrakasan, A.P.; Balakrishnan, H. An Application-Specific Protocol Architecture for Wireless Micro mesh Networks. IEEE Trans. Wirel. Commun. 2002, 1, 660–670.

[26] Lindsey, S.; Raghavendra, C.S. PEGASIS: Power-Efficient Gathering in Mesh Information Systems. In Proceedings of the Aerospace Conference, Big Sky, MT, March, 2002; pp. 1125–1130.

[27] Ayon Chakraborthy,Swarup kumar Mitra,Mrinal Kanti Niskar:A Genetic Algorithm Inspired routingProtocol for Wireless mesh Network: in International Journal of Computational IntelligenceTheory and practice,Vol 6No.1 June 2011

[28] C. Intanagonwiwat, R. Govindan, and D. Estrin,"Directed diffusion: a scalable and robust communication paradigm for mesh networks," Proceedings of ACM MobiCom '00, Boston, MA, 2000, pp. 56-67.

[29] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Mesh Networks," in the Proceedings of the First Workshop on Mesh Networks and Applications (MANETA), Atlanta, GA, October 2002.

[30] F. Ye, A. Chen, S. Liu, L. Zhang, "A scalable solution to minimum cost forwarding in large mesh networks", Proceedings of the tenth International Conference on Computer Communications and Networks (ICCCN), pp. 304-309, 2001.

[31] N. Sadagopan et al., The ACQUIRE mechanism for efficient querying in mesh networks, in the Proceedings of the First International Workshop on Mesh Network Protocol and Applications, Anchorage, Alaska, May 2003.

[32] V. Rodoplu and T. H. Meng, "Minimum Energy Mobile Wireless Networks", IEEE Journal Selected Areas in Communications, vol. 17, no. 8, Aug. 1999, pp. 133344.

[33] Shurman,M.M.; Al-Mistarihi, M.F. ; Mohammad, A.N. ; Darabkh, K.A. and Ababnah, A.A.," Hierarchical clustering using genetic algorithm in wireless mesh networks", Published in : Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention, Print ISBN: 978-953-233-076-2,May 2013.

[34] Lin Liu et.al , "Improvement of AODV Routing Protocol with QoS Support in Wireless Mesh Networks", Elsevier, Vol. 25, 2012.

[35] Malkhede, D. and Selokar, P., "Sybil Attack Detection in Mobile Adhoc Network", International Journal of Computer Science and Network, Vol. 4, Issue 3, 2015, pp. 469-474.

[36] Joshi, N. and Challa, M., "Secure Authentication Protocol to Detect Sybil Attacks in MANETs", International Journal of Computer Science & Engineering Technology, Vol. 5, No. 6, 2014, pp. 153–157.

[37] Mulla, M., "Efficient Analysis of Lightweight Sybil Attack Detection Scheme in Mobile Ad hoc Networks", IEEE International Conference on Pervasive Computing, 2015, Pune, India, pp.124-130.

[38] Alvisi, L., Clement, A. and Panconesi, A., "SoK: The evolution of Sybil defense via social networks", IEEE Symposium on Security and Privacy, Vol. 21, No. 2, 2013, pp. 382–396.

[39] Lee, P., Clark, A., and Bushnell, L., "A Passivity Framework for Modeling and Mitigating Wormhole Attacks on Networked Control Systems", Transactions on Automatic Control, Vol. 59, No. 12, 2014, pp. 3224–3237.

[40] Donga, P. and Joshi, S., "A Review On Trust Based Method To Detect Black Hole Attack In MANET", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, No. 6, 2016, pp. 728-732.

[41] Biswas, J., Gupta, A. and Singh, D., "WADP: A Wormhole Attack Detection and prevention Technique in MANET using Modified AODV routing Protocol", Information Communication and Embedded Systems, Vol. 16, No. 3, 2008, pp. 1078–1085.

[42] Dutta, C. and Biswas, U., "Specification based IDS for Camouflaging Wormhole Attack in OLSR", IEEE 23rd Mediterranean Conference on Control and Automation, 2015, Torremolinos, Spain, pp. 960–966.

[43] Kavitha, P., Keerthana, C. and VivekaNandhan, V., "Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network", International Journal of Communication and Computer Technologies, Vol. 2, Issue 2, 2014, pp. 4-9.

[44] Patidar, K. and Dubey, V., "Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks", Transactions on Parallel and Distributed Systems, Vol. 54, No. 7, 2014, pp. 93-102.

[45] Lee, Joon-Woo, and Ju-Jang Lee. "Ant-colony-based scheduling algorithm for energy-efficient coverage of WSN." IEEE Sensors Journal 12, no. 10 (2012): 3036-3046.

[46] Patel, Rajesh, Sunil Pariyani, and Vijay Ukani. "Energy and throughput analysis of hierarchical routing protocol (LEACH) for wireless sensor network." International Journal of Computer Applications 20, no. 4 (2011).