Intrusion Detection in MANET using Self Organizing Map (SOM)

V. Dinesh Kumar
Department of CSE
Kalasalingam University, India
velloredinesh78@gmail.com

Dr. S. Radhakrishnan
Department of CSE
Kalasalingam University, India
srk@klu.ac.in

Abstract - **Mobile Ad-hoc networks (MANET) are formed with dynamism and upheld by individual hosts in a network. In these type of networks all communication occurs through a wireless medium and the nature of the network is decentralized and dynamic. Hence it probes for a number of security problems and in order provide security against malicious attacks, Intrusion Detection System (IDS) is commonly used as a second route of protection in MANET. Intrusion detection models are used to detect the attacks based on the patterns and alerts in case of intruders are being met with the system. In this paper, we propose and implement intrusion-detection system grounded on artificial neural network model such as Self-Organizing Map (SOM) based competitive network, which in turn plays a vital role in detection of malicious nodes based on input data patterns. The proposed model deals with different types of attacks and their detection approach based on SOM model. The approach aids at increasing Detection rate as well as reducing the False alarm rate, which in turn helps to detect those attacks before it makes larger damage to the network and prevent them with supportive techniques and increase the network performance. The experimental results of proposed model is evaluated under different parameters.**

Keywords: artificial neural network, Detection rate, False alarm rate, Intrusion detection, MANET, security, SOM.

I. INTRODUCTION

Mobile ad-hoc networks (MANETs) are dynamic in nature. The characteristics are generally: exposed noble-to-noble [2], related wireless standard, rigid means of controls and extremely active system topology and hosts directness to somatic seizure. Due to its nature it supports variety of applications such as portable processing, quest and liberate, calamity rescue, [4] but the approach of fortifying MANETs is quiet in its embryonic stage. Equated through a stationary system, a MANET is further susceptible en route for its limited features, for example exposed standard, on the go topology, reserve restrictions, and absence of consolidated supervision. Certainly, a diversity of assaults battered the system level, like Black Hole [5] and Gray Hole stabbings, besides these are being recognized in addition deliberated in these works. In several spasms, invaders introduce themselves on the route among the basis and end point, by this means governing the complex transportation stream.

Routing protocols plays an important role in MANETs. Amid of several course-plotting conventions that are been industrialized towards tolerating identity-organizing and nature-retaining transmitting in MANETs, the Ad-hoc On-demand Distance Vector (AODV) protocol [1] have been developed to be one of the best prevalent. Accordingly, there are numerous assault headings in AODV which permit assailants to upset its course revelation and bundle sending methods. In the part of dodging the impacts of vindictive exercises [3], systems are important to in any event reduce such impacts. Interruption location frameworks (IDs) might be utilized as one of these creations. Interruption Detection System (IDS) are regularly called as second line of safeguard, has gotten critical and matching part in securing Manets. Interruption is any assembly of activities that endeavor to coordinate the trustworthiness, privacy, or accessibility of a store and an interruption identification framework (IDS) [6] is a framework for the disclosure of such interferences. An IDS uncovers conceivable damages of a security system by watching framework exercises. In the event that an occurrence might be recognized a response could be acquainted with obstruct or diminish the debilitation to the framework. There are three primary interruption identification approaches [7, 28]: irregularity based; abuse based; and determination based. An aberrance based framework diagrams the evidences of standard exercises of the framework, for example, summon demand frequencies and CPU utilization for arrangement. It faculties intrusions as aberrances, i.e. variations from the norm from made ordinary practices. Abuse based finding likens known event signs with current framework occasions. It is for the most part picked by suitable Idss since it is generally composed and has a squat false positive rate. With particular based styles a set of confinements of a project or a meetings are specified and interruptions are recognized as runtime harms of these particulars. They pool the benefits of abnormality based and abuse based location works on, giving recognition of known and obscure events with more level false positive rate. An assorted qualities of routines have been utilized to gadget irregularity recognition, e.g. factual systems, and counterfeit consciousness [6] frameworks like information mining and neural frameworks.

Neural Networks [25] is a study territory with various points of interest that have not been oppressed in impromptu systems. We abuse their primary plusses in the configuration of an interruption discovery motor, which is some piece of a neighborhood IDS substitute. The impulse of this paper is the interruption recognition motor that is dependent upon a sort of neural systems known as Self-Organizing Maps (SOM). Kohonen's Soms are a sort of unsupervised taking in. The point is to learn some causal course of action of the information Kohonen's SOM [8] is known as a topology-

978-1-4799-4989-2/14/$31.00 © 2014 IEEE

protecting guide subsequent to there is a topological erection exacted on the hubs in the framework. A topological guide is essentially a plotting that jelly area co operations. Self-organizing Map (SOM) is used to detect connection anomalies, and limit malicious nodes. Detection of malicious nodes alone will not solve the problem of network, one must able to prevent those attacks from the network to make the network more secure. There are numerous techniques available to prevent attacks from a network, among them cryptographic techniques have an upper hand.

II. RELATED WORK

Due to the systems open medium, decentralized architecture and several other features makes the environment vulnerable to several attacks and damages the normal functionality of the network. The survey includes analysis of various attacks in MANET. In MANETs routing protocols [10] plays a major role in discovering the next hop as well as routing of packets between source and destination, but these routing protocols are not secured. For example In Ochola et.al [11] evaluated the risks caused by Black hole attack in MANETs with respective to AODV protocol and also the counter measures to overcome using ideal threshold values of anomaly detection approach. In Ayday et.al [13] investigated the ability of routing protocols in establishing trust bond between both the nodes in a network as well as the effects and proposed Dynamic Bayesian model in order to provide security with respect to Secretive (insider) attacks. Apart from several counter measures techniques there are other methods such as Intrusion Detection that are considered as second line of defense in security system plays a vital role in detecting attacks w.r.t MANET. There are several approaches such as Adnan et.al [14] observed that these wireless networks prone to various attacks in network layer that causes damage to the system functionality and reduces the network performance and to regulate this process they specified Interruption Detection & Adaptive Response instrument (IDAR) that utilizes a synthesis of both abnormality based and learning based interruption discovery strategies helps identify ambushes and decrease them.

In Christos et.al [15] identified various intrusion detection systems as well as analyzed the security and performance of all those systems w.r.t to a different attacks and changes in the network are summarized. In Ming et.al [5] observed the changes of an ad-hoc network and the security attacks such as Black hole and suggested ABM (Anti-Black hole Mechanism) function which helps the intrusion detection system to identify and secure the system. In Adrian et.al [16] has suggested an IDS system that helps to reduce the resource consumption in networks such bandwidth and delay. The proposed approach includes the use of Hybrid IDS that helps to overcome the defect in detection and prevention methods of existing approach. In John et.al [3, 9] identified the limitations in building an efficient IDS model in order to detect and prevent a network from different security attacks and increase the performance. The proposed model includes three main prototypes of IDS design, namely, rational rule-based systems, selective valuation built methods as well as numerical grouping methods. In Joao et.al [17] revised various approaches that relates the clustering schemes as well as machine learning to detect anomaly to satisfy this approach the model includes IDS designed with recipient working attributes (ROC) bends and the relating territory under the ROC bend (AUC) measurements for different operational conditions serves to build exactness and productivity of system which is inspected under diverse assaults.

In Chris et.al [18, 23] revised the model of sink hole attack in MANET as well as their network performance and developed Sink Intrusion Detection System to overcome the approach. Artificial neural networks plays an important role in any field of networks as such its implications are used in MANETs in order to design security frameworks along with intrusion detection systems. The existing models are Shahaboddin et.al [19, 24] conveyed the approach of developing an IDPS with the help of artificial computational intelligence called collaborative-based wireless IDPS (Co-WIDPS) which includes the use of Fuzzy rule approaches with different mechanisms for detection of attacks with low rates. In Wei et.al [8,26] studied the need for efficient security frame work for MANETs in order to detect a range of attacks and increase the performance hence they proposed an intrusion detection system with the approach of neural networks algorithm such as Self Organizing Maps (SOM) are used to analyze w.r.t energy and delay. In Sergio et.al [20.24] and Pedro suggested a range of different classification algorithms that are efficient in developing an IDS to detect a range of attacks with lower rates when compared to other systems and increase the performance. In Mazhar et.al [21, 25] and Farooq proposed an IDS based on Artificial Immune System (AIS) with the use of Bee Ad-hoc system that helps to detect the attacks with higher accuracy and lower false positive ratio.

III. INTRUSION DETECTION IN MANET

Remote Ad-hoc Networks, habitually called as portable impromptu systems (Manets), manages the capacity of including a few hubs without a focal access point. Remote specially appointed systems need to be ensured, interruption recognition frameworks (IDS) [24] are utilized for uncovering heretic door focuses. On a succeeded wireless network, a unified network technique is used to test the radio occurrences of the network and reports reprobate access-sockets. To a MANET [8, 6], an interruption recognition classification resolution needs to be employed on a host based system to thwart network attackers. Conservatively, an intrusion detection system will use a MAC address to recognize the joining access points and associate it with a list of permitted access points. This is a flaw in the meantime rogue devices can skit MAC addresses. Modern operations for a wireless ad-hoc network intrusion detection system will use inventory facts which will decide between normal and abnormal usage of the network's possessions.

A. Intrusion Detection System

The configuration of IDS [21] utilized within impromptu systems could be either appropriated or agreeable or dispersed and progressive. The unlucky deficiency of focal watching hubs and the absence of dependence between honorable hubs of a remote impromptus system focus on a need for focal interruption recognition framework. The strewn and various leveled IDS are grounded on differentiating the versatile impromptu system into groups. Despite the fact that group

based IDS [3, 17] have the profit of more level disclosure work, the methodology of making groups and select bunch heads may attach to a tremendous issue. Despite the fact that, the vicinity of group heads and the apparent danger of their usage by malicious intruders decay the evaluated security. Moreover, the strewn and classified IDS are more successful for impromptu systems with truncated versatility. Consequently, the steady and animated environment of impromptu system proposes that the interruption location framework ought to be strewn and strong. Every projection of the specially appointed system need to finish its local interruption recognition utilizing accessible data at its separate positions. Similarly, the backing between IDS substitutes ought to be held through secure channels Each IDS operator is made out of the accompanying parts:

1) Data Collection & Analysis: The model includes creating a MANET scenario and analyzing the performance of a network as well as simulating various attacks and again check the network status and the analysis is liable for selecting the required information needed to analyze the behavior of network. The data being gathered includes the following namely Source node Id, Destination node Id, Protocol value, Delay value, Root node Id, Packet Delivery Ratio.

2) Intrusion Detection Process: is accountable for sensing local irregularities using the data. The local anomaly detection is performed using the SOM [8, 26] neural network model. The procedure that is followed in the local detection engine is the one described below:

a) Select categorized data and execute the applicable alterations.

b) Calculate the model by means of training data and the SOM model.

c) Apply the model to check information in order to sort it as regular or irregular. Such that the SOM model will generate maps which holds the differences between the data provided.

The similar approach is carried out at each node in the network. If any abnormalities are found in these process the respective warnings will be generated based on the seriousness of the attack and respective prevention systems will be modelled for prevention of the network.

IV. SELF-ORGANIZING MAPS

The Self-Organizing Maps (SOM), for the most part recognized as Kohen's framework is a computational plan for imagining and investigation of rich-geometric data, particularly for logically accomplished detail. SOM or organizing toward oneself characteristic guide (SOFM) [22] is a sort of fake neural system that is master in utilizing unmanaged figuring out how to yield a squat-geometric (characteristically 2d), discretized outline of the investment space of the preparation models, entitled as a guide. Organizing toward oneself maps are disparate from previous simulated neural systems in the rationale that they utilize a district assignment to circle the topological stakes of the interest range. Indistinguishably most extreme counterfeit neural systems, Soms works in two methodologies, for example, staying in shape and plotting. Preparing structures the plot utilizing investment examples. It is an unassuming methodology, additionally termed as way aligned. Plotting mechanically composes another info way. An orchestrating toward oneself guide includes constituents named as hubs or neurons.

The approach of Self-Organizing Maps structure is depicted in the above format. Related with each node is encumbrance route of the similar aspect as the input information routes and a point in the plot. The typical organization of nodes is a systematic layout in a sextet or ellipsoidal lattice. The self-organizing map labels a plotting from a surpassing geometric input are a to a minor geometric plot area. The practice for retaining an angle from information area onto the plot is to find the node with the adjoining density angle to the angle taken from information area and to allocate the plot organizes of this node to our angle.

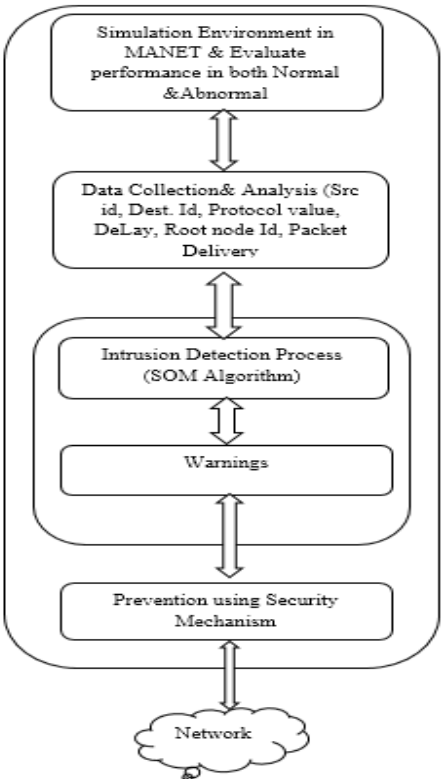

Fig .1. Model of Intrusion Detection in MANET [1]

A. Learning Phase of SOM

The target of learnedness in the masterminding toward oneself guide [8] is to foundation different segments of the framework to answer likewise to guaranteed info designs. This is moderately determined by how graphical, acoustic or other tangible detail is held in detached allotments of the savvy cortex in the mortal personality. The heaps of the neurons remain introduced specific to piddling subjective values or tested reliably from the subspace navigated by the two heading prime constituent Eigen courses. With the later exchange, taking in is plentiful faster on the grounds that the preparatory loads as of recently give a great estimation of SOM [27] loads. The system must be served to a substantial

heft of specimen courses that outlines, as close as likely, the classes of ways foreseeable through plotting. The examples are generally controlled various times as reiterations. The readiness misuses practical taking in. At the point when a worked out example is served to the system, its Euclidean separation to all heap ways is computed. The neuron whose mass trajectory is practically like the reaction is entitled as the Best Matching Unit (BMU) [8]. The masses of the BMU and neurons close to it in the SOM framework are usual towards the information trajectory. The scale of the alteration diminishes with time and separation (inside the grid) from the BMU. The upgrade strategy for a neuron with weight trajectory Wv(s) is

$$Wv(s + 1) = Wv(s) + \Theta(u, v, s)\, \alpha(s)(D(t) - Wv(s)) \quad (1)$$

Where s is the stair index t is bolstered alongside the preparation model, u is the list of the BMU for D(t), α(s) is a monotonically declining taking in steady and D(t) is the data trajectory; v is required to call all neurons for each importance of s and t. Subject to the requisitions, t can test the preparation information set. The region errand Θ (u, v, s) rest on the casing space around the BMU (neuron u) and neuron v. In the unstudied framework it is 1 for all neurons close plentiful to BMU and 0 for others, however Gaussian errand is a mutual perfect as well. In any case of the useful structure, the region errand diminishes with time. At the beginning state when the region is expansive, the orchestrating toward oneself happens on the aggregate ruler. At the point when the region has minimized to reasonable a couple of neurons, the masses are uniting to nearby estimates. In a few provisions the taking in variable α and the region capacity Θ falls continuously with total s, in others they diminish in step-wise technique, one for each T steps. This system is dreary for each one info trajectory for various set.

The system winds up relating yield hubs with groups or clusters in the information data set. In the event that these shows could be entitled, the titles might be focused on the related hubs in the expert net .over the span of speaking to, there will be one winning neuron that is the neuron whose heap trajectory falsehoods neighboring to the information trajectory. This might be unfaltering by processing the Euclidean space around data trajectory and weight trajectory. Although implying info information as trajectories has been highlighted it ought to be prestigious that any sort of substance which might be portrayed numerically, which has a pertinent store sum going with it, and in which the vital methods for preparing are possible could be utilized to make an orchestrating toward oneself guide. It holds frameworks, consistent capacities or considerably other masterminding toward oneself maps.

B. *Self-Organizing Map based Intrusion Detection in MANET*

Mobile Ad-hoc Networks are categorized as one of the best approaches of wireless networks. This is because of its characteristics that support for any situation and also easy to deploy as well as its open medium supports for any host to join and leave the network based on its characteristics. But MANETs doesn't provide the assured security between the host in communication process due to its open medium and decentralized architecture. Hence in order to provide secure communication it is focused on various approaches among them Intrusion Detection plays a key role in detecting various security attacks and helps to prevent them. In order to detect attacks there are several detection approaches but they doesn't get better results. Hence in directive to convey out the approach of intrusion detection we specify the use of Neural network models [8, 20] such as Self-Organizing Maps [27] that helps to easily detect based on the input patterns and its output representation clearly specify whether it is normal or malicious data which incurs vey less time to detect and with lower detection rates making the computation more feasible.

The proposed model incurs the use of SOM model used to detect attacks based on training and initiation phase that progress to results along with weight vectors. The proposed SOM model states the approach of allocation of weight as well as training process and detection of various malicious activities. In the model for every input all the neurons determine their activation functions and the neuron with lower activation function is declared as winner. The model that contains both the winner and neighboring neurons adjust their weights such that they can respond to a better similar input in future. The model of SOM is carried out with the classical steps stated as follows at each and every stage before the start of detection of malicious nodes.

1) Initially each participating neuron is associated with their respective weights, and then choose random vectors for training the SOM.

2) Calculate the Best Matching Unit (BMU) based on Euclidean distance of the neurons weights (W1, W2… Wn) and the input vectors (V1, V2… Vn) values.

3) Euclidean distance is nothing but measurement of similarity between two sets of data.

$$\text{Dist.} = \sqrt{\sum_{i=0}^{i=n} (Vi - Wi)^2} \quad (2)$$

4) An aggressive corrosion function that decreases on each monotony until the vicinity is BMU itself. It can be specified as exponential decay function.

$$\sigma(t) = \sigma_0 \exp\left(-\frac{t}{\lambda}\right) \quad (3)$$

Where

$\sigma(t) = width\ of\ Lattice\ at\ time't'$

$\sigma o = width\ of\ lattice\ at\ time't0'$

$\lambda = Time\ constant$

5) The new weights of the neuron is old weight plus a fraction of difference between old weight and input vector. Eq. (1)

6) The effect of location is defined by a Gaussian curve so that the neurons closer are influenced more than farther neurons.

$$\Theta(t) = \exp\left(-\frac{dist^2}{2\sigma^2(t)}\right) \quad (4)$$

Where $\theta(t) = \text{influence rate}$

$2\sigma^2(t)$=width of lattice at time't' for any given neuron.

Repeat from step 2 for convergence.

The approach is more over used to detect attacks and also helps in identification as well as prevention of the attack. In

this approach inputs to the SOM are collected during the simulation process which are collected using traces. Which includes both for the normal and malicious behavior respectively.

V. SIMULATION STUDY

The core objective of this effort is to analyze the enactment of Self-Organizing Map (SOM) while exasperating to discover falsified activities that might ensue in MANETs. The performance of all these approaches helps analyzes the effects of security in an ad-hoc network.

A. Simulation Environment

In order to assess the method we have virtualized Mobile Ad-hoc Network (MANET) and the process followed with a series of experiments. The approach is carried out with the hypothesis that the network has no established architecture and engaged Ad hoc On Demand Distance Vector (AODV) for routing. We executed the simulation using NS2 (Network Simulator) tool. Along with this approach the similar attacks are being executed with varying malicious nodes in the network for each attack.

TABLE 1.SIMULATION PARAMETERS

Parameter	Value
Simulator	NS-2.34
Number of Nodes	50
Simulation run time	600 sec
Area	950x850 meters
Movement	All Nodes
Mobility	5,10,15,20 m/s
Simulation Traffic	CBR (Constant Bit Rate)
Routing Protocol	AODV
Queue Length	100
Network Traffic	2.0 mbps
Transmission range	250m

The approach includes the simulation of three different types of attacks such as:

1) Black Hole attack [11, 20]: In this violence a malevolent node sends forged routing information which leads to receive packets without forwarding them the malicious node drops them instantaneously. The simulation approach is carried out such that when a malevolent Black Hole receives a RREQ packets it immediately replies with RREP packets to the endpoint without inspection whether it has the route to the endpoint. As result the Black Hole node is the first protuberance to the source will send packets to it which in turn drops them without forwarding.

2) Packet dropping attack [12]: In the process of simulation of packet dropping attack a node is chosen as malicious such that the malicious node will drop all the RERR packets leading to authentic nodes which will result in forwarding packets to broken links.

3) Gray Hole attack [11, 12]: The approach of simulation includes the malicious nodes concentrates on one particular node or IP address such that it will drop all the data packets being forwarded to that particular node such as RREQ and RREP.

In these manner the above attacks are simulated and their respective performance is being analyzed. The simulation parameters are maintained constantly for all the attacks there by increasing the malicious nodes in case of Black Hole attack with respective to stimulation up to 5 malicious nodes are simulated with changes in existing AODV for all attacks.

B. Data Sets

A significant resolution is the feature vector choice that will be used in the Self-Organizing Map. The nominated structures [8] should be able to briefly characterize network action, while distinguishing the behavior among actual network and a network with attacks. The following selected features are with respect to network layer simulation.

1) Src ID: The node that acts as originator for Hello/Data packets in the network.

2) Dst ID: The node that acts as receive/reply for Hello/Data packets of source in the network.

3) Protocol: A set of rules and procedures that are used during the transmission of Hello/Data packets in the network.

4) Delay: Indicates the network position when a particular Hello/Data packet is lost during transmission.

5) Root ID: Indicates the nodes that successfully transmit a packet to other nodes in the network.

6) Packet Delivery Ratio: Indicates the network performance based on number of packets being transferred between both parties in a network during communication.

The information of all these data sets can be extracted from traces and it would be used for SOM classifier. These structures should be transformed in a way such that it will suit with SOM input function. Normally, the data is being converted into series of decimal values. During the process of testing the initial feature vectors can be adjusted to get better results.

C. SOM structure

The approach is carried out with linear structure of SOM [27], which maps the given patterns onto the available cluster units. The winning neurons along with the neighboring distances between the neurons are being updated frequently based on winning neuron information. There are a total of 36 output neurons in the experiment. The winning neuron [8] represents the one with shortest distance associated with each neuron.

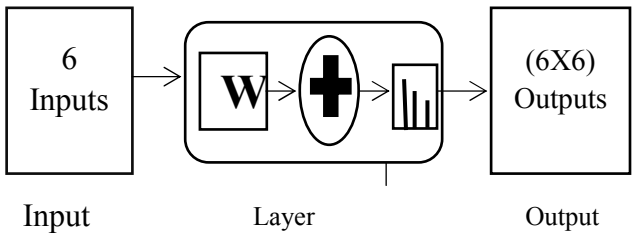

Fig.2.Model of Self-Organizing Map [8]

Since there are six inputs the output neurons size will be 36 which holds all the data of those six inputs including its weights, neighborhood vector values are being involved in it. The above figure represents overall functionality of network process. During layer functionality the weights along with its equivalent representation bias values are being used which yields better output with varying bias values. The output represents the results in various forms with respect to the input based on training set data.

D. Experimental Results

In the experiment we match the enactment of MANETs with respective to different attacks such as Black Hole attack [11], Packet dropping attack, Gray Hole attack similarly others also with respect to the network layer. The below figures are used to address the behavior of network under these attacks.

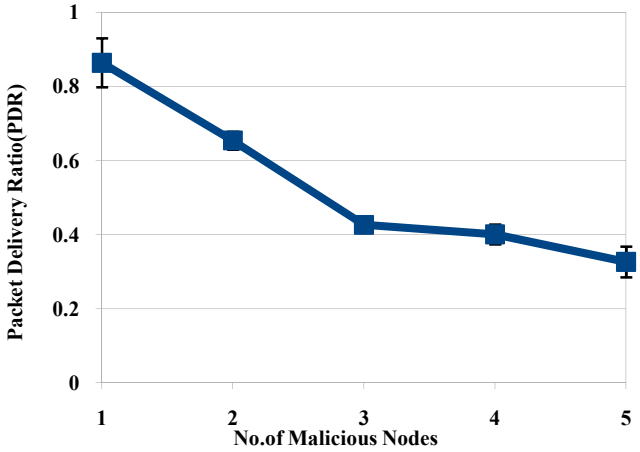

Fig.3. Graph showing the degrading performance of Packets that being sent/received with respect to increase in no.of malicious nodes in Black hole attack.

The figure3 represents the performance of network such that when number of malicious nodes increases it leads to dropping of packets during transmission such that the packet delivery ratio also decreases.

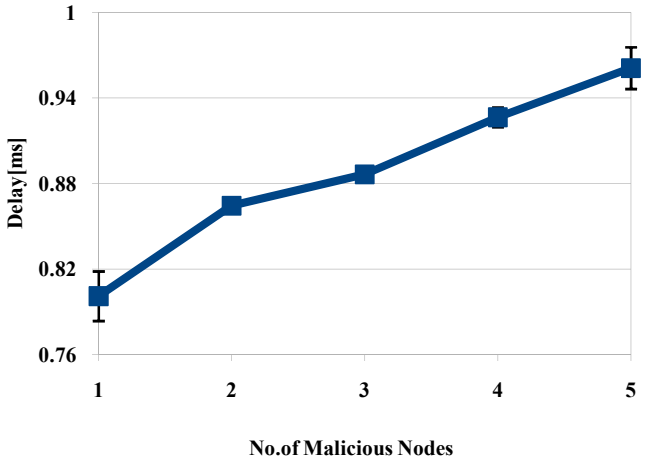

Fig.4. Graph showing the degrading performance of a network as the end-to-end delay in the network grows with respect to increase in no.of malicious nodes in Black hole attack.

The figure 4 represents the performance of network such that when number of malicious nodes increases the delay value also increases causing the network to split or abort the transmission.

The same approach can be seen for Gray Hole [11] attacks as if the malicious nodes drops some data packets from particular nodes targeted at some particular time only. The next process includes the results that helps to identify the malicious nodes according to data sets that are used for training and testing under different conditions with changing bias values to get better results that are being compared with existing neural network models.

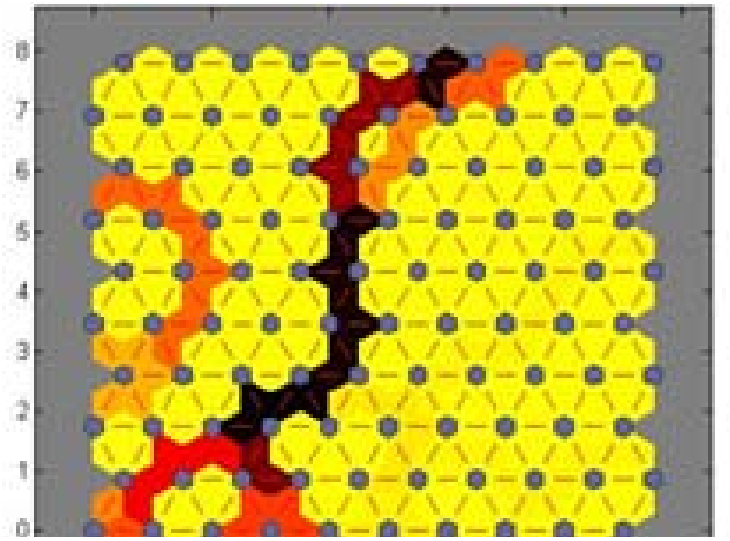

Fig. 5(a) Neighboring weight distance

The figure5(a) represents the neighbouring weight distance between two regions that are formed.Lighter color represents short distances and darker color represents larger distance,a band of dark segments that streches from lower region to upper region depicts the signifance of an attack in the entire SOM network based on the number of neighboring nodes

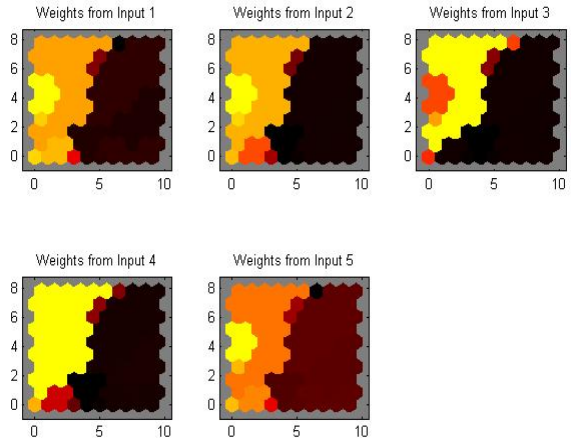

Fig. 5(b) Weights assigned for each input vector

The figure 5(b) speaks to a weight plane for every component of the info vector. They are visualizations of the weights that associate each one info to each of the neurons. On the off chance that the association examples of two inputs were fundamentally the same, such that the inputs are exceptionally associated. Which in turn helps to identify the proportion of attack with color difference.

The figure 5(c) represents detection of three malicious nodes as well as changes in the weights in respective to data vectors along with mapping neurons. The graph with darker color depicts the new updated weights w.r.t to attack detection with higher weights.

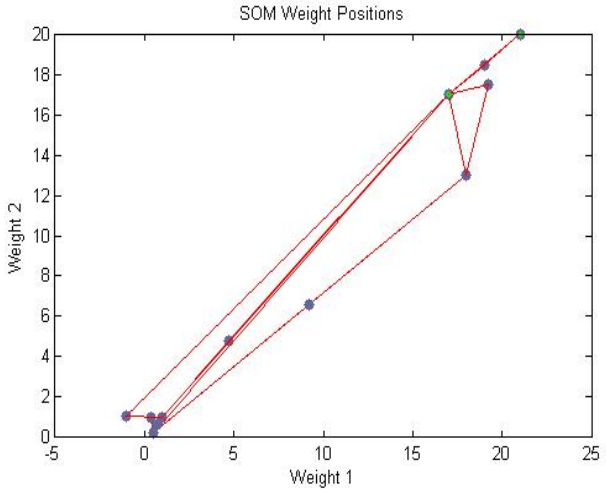

Fig. 5(c) Weight positions of neurons

The above features helps to detect and identify the intrusions over the network and founds to be reliable. The approach is tested for various data sets ranging to nearly 50 different data sets comprising different attacks. The SOM [26] approach is found to be more reliable because of its competitive nature. The outputs in each of the approach are being used for detecting the performance which is being measured in terms of Detection rate and False Alarm rate [26, 28]. These values helps to identify the number of attacks by the Intrusion detection system with respect to training data as well as no. of data sets affected by the malicious nodes with respect to normal data.

TABLE.2. DETECTING PERFORMANCE

No.of Malicious nodes	**Detection Rate (%)**		**False Alarm Rate (%)**	
	MLP[20]	***Proposed***	***MLP[20]***	***Proposed***
1	77.01	90.130	0.05	0.051
2	76.23	89.096	0.21	0.142
3	72.67	89.021	0.26	0.101

The table 2 indicates the detection rate of particular attack when malicious nodes are increasing. The proposed model is compared with MLP [20] which shows difference in the performance of network w.r.t the detection rate and false alarm rate in the proposed system.

Apart from alerts in the Intrusion detection system this approaches clearly helps to identify the attacks as well as their false rates with which it will be possible to prevent them using security mechanism and also increase the network performance as well as avoid a wide range of problems and can be able to avoid some bottleneck problems in MANET.

VI. CONCLUSION & FUTURE WORK

In this paper, we presented a unified framework for anomaly detection scheme based on Self-Organizing Map. This approach was achieved by hosting a network routine design scheme that overtakes the existing security models which are designed based on resource constrained network. Since information of network topology plays an important role in monitoring network performance as such approaches favors a lot of attacks which in turn helps to capture the existing data packets in the network and cause loss of information. The proposed approach uses neural network techniques for intrusion detection which helps for easier detection of those attacks with alerts. The experimental results achieved in this model is found to be better when compared with other neural network techniques in terms of detection rate and false alarm rate. The future work model includes collection of real time data and use effective security mechanisms to prevent the attacks and increase network performance.

REFERENCES

[1] Adnan Nadeem, Michael P. Howarth, "An intrusion detection & adaptive response mechanism for MANETs," *Ad-hoc Networks*13 (2014) 368-380.

[2] Jan von Mulert, Ian Welch, Winston K.G. Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV," *Journal of Network and Computer Applications* 35 (2012) 1249–1259.

[3] John Felix Charles Joseph, Amitabha Das, and Boon-Chong Seet, Bu-Sung Lee, "Opening the Pandora's Box: Exploring the fundamental limitations of designing intrusion detection for MANET routing attacks," *Computer Communications* 31 (2008) 3178–3189.

[4] Da Zhang, Chai Kiat Yeo, "Distributed Court System for intrusion detection in mobile ad hoc networks," *computers & security* 30 (2011) 555-570.

[5] Ming-Yang Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," *Computer Communications* 34 (2011) 107–117.

[6] Aikaterini Mitrokotsa, Christos Dimitrakakis, "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection," *Ad Hoc Networks* 11 (2013) 226–237.

[7] SevilSen, John A. Clark, "Evolutionary computation techniques for intrusion detection in mobile ad hoc networks," *Computer Networks* 55 (2011) 3441–3457.

[8] Wei Wanga, Huiran Wang, Beizhan Wang, Yaping Wang, Jiajun Wang, "Energy-aware and self-adaptive anomaly detection scheme based on network tomography in mobile ad hoc networks," *Information Sciences* 220 (2013) 580–602.

[9] Eugene Y. Vasserman and Nicholas Hopper, "Vampire attacks: Draining life from wireless ad-hoc sensor networks," *IEEE Transactions on Mobile Computing* Vol.12 No.2 (2013) 1-15.

[10] Radu Stoleru, Haijie Wu, Harsha Chenji, "Secure neighbor discovery and wormhole localization in mobile ad hoc networks," *Ad Hoc Networks* 10 (2012) 1179–1190.

[11] Ochola EO, Eloff MM, "A Review of Black Hole Attack on AODV Routing in MANET," *IEEE Transactions on Mobile Computing* Vol.12 No.2 (2012) 1-8.

[12] Praveen Joshi, "Security issues in routing protocols in MANETs at network layer," *Procedia Computer Science* 3 (2011) 954–960.

[13] E. Ayday, F. Fekri, "A protocol for data availability in Mobile Ad-Hoc Networks in the presence of insider attacks," *Ad Hoc Networks* 8 (2010) 181–192.

[14] Adnan Nadeem and Michael P. Howarth, "An Intrusion Detection & Adaptive Response Mechanism for MANETs," *Ad-hoc Networks*11 (2013) 1-28.

[15] Christos Xenakis, ChristoforosPanos, IoannisStavrakakis, "A comparative evaluation of intrusion detection architectures for mobile ad hoc networks," *computers & security* 30 (2011) 63-80.

[16] Adrian P. Lauf, Richard A. Peters, William H. Robinson, "A distributed intrusion detection system for resource-constrained devices in ad-hoc networks," *Ad Hoc Networks* 8 (2010) 253–266.

[17] Joao B.D. Cabrera, Carlos Gutierrez, Raman K. Mehra, "Ensemble methods for anomaly detection and distributed intrusion detection in Mobile Ad-Hoc Networks," *Information Fusion* 9 (2008) 96–119.

[18] H. Chris Tseng, B. Jack Culpepper, "Sinkhole intrusion in mobile ad hoc networks: The problem and some detection indicators," *Computers & Security* (2005)24, 561-570.

[19] Shahaboddin Shamshirband, Nor BadrulAnuar, Miss Laiha Mat Kiah, Ahmed Patel, "An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique," *Engineering Applications of Artificial Intelligence* 26 (2013) 2105–2127.

[20] Sergio Pastrana, Aikaterini Mitrokotsa, Agustin Orfila, Pedro Peris-Lopez, "Evaluation of classification algorithms for intrusion detection in MANETs," *Knowledge-Based Systems* 36 (2012) 217–225.

[21] N. Mazhara, M. Farooq, "A hybrid artificial immune system (AIS) model for power aware secure Mobile Ad-Hoc Networks (MANETs) routing protocols," *Applied Soft Computing* 11 (2011) 5695–5714.

[22] Nikos Komninos, Dimitris Vergados, Christos Douligeris, "Detecting unauthorized and compromised nodes in mobile ad hoc networks," *Ad Hoc Networks* 5 (2007) 289–298.

[23] Bounpadith kannhavong, Hidehisa Nakayama, Yoshiakine moto, Andneikato, "A Survey Of routing attacks In Mobile ad-hoc networks," *IEEE Wireless Communications* (2007) 85-91.

[24] Nabil Ali Alrajeh and J. Lloret, "Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks* (2013) 1-6.

[25] S. Ganapathy, P. Yogesh, and A. Kanna ,"Intelligent Agent-Based Intrusion Detection System Using Enhanced Multiclass SVM," *Computational Intelligence and Neuroscience* (2012) 1-10.

[26] Aikaterini Mitrokotsa, Nikos Komninos and Christos Douligeris, "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET," *IEEE computer society* (2008) 1-10.

[27] A.Ultsch, H.P. Siemon "Kohonen's SeIf Organizing Feature Maps for Exploratory Data Analysis," 305-308.

[28] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE, "EAACK—A Secure Intrusion-Detection System for MANETs," *IEEE Transactions on Industrial Electronics,* Vol. 60, No. 3, March (2013) 1089-1098.