An Effective Intrusion Detection System for Routing Attacks in MANET using Machine Learning Technique

Pratik Gite
Ph.D. Scholar
PAHER University
Udaipur (R.J.), India

Sanjay Thakur, Ph.D.
Associate Professor
PAHER University
Udaipur (R.J.), India

ABSTRACT
Wireless communication is widely adopted and application oriented technology **T**here are a huge literature about Mobile Ad-hoc network is available. In these studies, the ad hoc network has two major issues security and performance. In this paper a feasible and adoptable solution is introduced for enhancing security in MANET. The presented work utilizes the network characteristics and their behavioral difference during attack. Using the attack and normal network behavior a machine learning algorithm is trained and the malicious patterns are distinguished according to the new network samples. The proposed machine learning based ad hoc network security is implemented using NS2 simulator and the performance of the system is evaluated in terms of metrics viz. throughput, packet delivery ratio, end to end delay and energy consumption. According to the obtained results the performance of the proposed secure network is optimum and adoptable.

General Terms
Security, Intrusion Detection System, Performance Analysis

Keywords
MANET, NS-2, Packet Delivery Ratio, Routing Overhead, End to End Delay, Energy Consumption, Machine Learning Technique

1. INTRODUCTION
In wireless networks the mobile ad hoc network is much promising and area of research and development. Mobile ad hoc network is dynamically organized group of network nodes which performing the communication. In different literatures there are two key issues are observed first performance and secondly the security. In this presented work the mobile ad hoc network is investigate the security issues and trying to develop the efficient and secure network communication. Basically the network topology and route discovery is organized using the routing protocols [1].

Thus mobility is a major issue in performance additionally the adoptive nature of the routing protocols make it poor against the security flaws [2][5][14][15]. Therefore a new infrastructure based ad hoc network is proposed for designing secure and efficient communication. The security investigation is based on the routing based attack deployment techniques. Because most of the attackers are utilize the routing strategy for attack deployment.

Thus the following attacks are considered for investigation and security system design. These are Black hole attack, Wormhole attack Gray- hole attack, DDOS attack.

Table 1 Attack characteristics

S. No.	Attack type	Parameter
1	Black hole	1. Packet delivery ratio 2. buffer size
2	Wormhole	1. time to leave 2. packet delivery ratio 3. location estimation 4. buffer size
3	Denial of Service Attack	1. Control message 2. Energy 3. packet delivery ratio 4. buffer size
4	Gray hole	1. packet delivery ratio

In the above given network characteristics the mobile ad hoc networks traffic is invigilated and the traffic can be classified for malicious or normal activity. The next section includes the basic techniques and tools available for accurate pattern recognition. Using the optimum techniques the traffic classification is performed for malicious acting nodes.

2. BACKGROUND
According to the available literature a number of techniques using the KDD CUP 99's dataset classification the IDS (intrusion detection system) designed. This dataset is an effort of Lincoln Labs, who setting up an environment to acquire nine weeks of raw TCP dump data for a local-area network (LAN) simulating a typical U.S. Air Force LAN. They operated the LAN as if it were a true Air Force environment, but peppered it with multiple attacks.

In order to classify this data a number of machine learning and data mining based techniques are available. These data model analyse the KDD CUPs traffic data and classify traffic input patterns into their actual patterns. In order to develop such kind of data model the following algorithms are frequently utilized for learning and identifying the attack pattern [6] [8] [17].

1. KNN: KNN (k-nearest neighbour) algorithm is an unsupervised classification technique. This method finds the distance between two different instances of data and groups them according to the minimum distance basis.

2. SVM: SVM is also termed as the support vector machine that is a supervised learning technique. Using a set of training samples each marked as belonging to some classes. An SVM algorithm develops a data model that classifies the patterns into a class or other. This property making it a non-probabilistic binary linear classifier, An SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall on.

3. BPN: back propagation neural network is also a supervised learning algorithm. That contains three layers namely input layer, hidden layer and an output layer. These layers are computes the weights for performing the classification. The detailed neural network is introduced in next section [3].

4. Bayesian classifier: Bayesian classifiers are the statistical classifiers. That is based on the Bay's probability theory. Bayesian classifier is able to analyse data and according to the obtained probability distribution predict class membership probabilities such as the probability that a given tuples belongs to a particular class.

5. Decision Trees: decision trees are transparent data model which can be evaluated using pen and paper. Thus the decision tree first analyse the data according to their class labels and then prepare a tree data structure for demonstrating the relationship among the available attributes and these attributes are help to identify the available pattern and their class label assignment.

This section provides the understanding about different technique that can use for pattern analysis and their identification. Next section includes detailed study of BPN algorithm.

3. BACK PROPOGATION NEURAL

The neural network is a supervised learning technique [21] [25]. That algorithm is widely accepted for effective and accurate pattern detection. Therefore a wide range of applications are utilizing the neural network for classification, prediction, pattern recognition. The neural network consist of three different layers first input layer, second hidden layer and third the output layer [22] [23]. During implementation of neural network, the input layer and hidden layers are implemented together using 2D vector and output layer is implemented using single dimensional array. The weight calculation is performed using input and hidden layers. And the output of neural network is stored in output layer [13] [18].

The implementation of neural network is defined in two phases' first training and second prediction: training method utilizes data and develops trained data model. This trained model is used for pattern detection.

2. Here first is a two dimensional array W_{ij} is used and output is a one dimensional array Y_i.

3. Original weights are random values put inside the arrays after that the output**.**

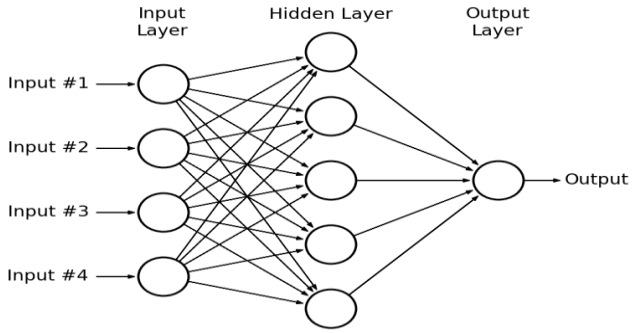

Figure 1 Neural Network

Training:

1. Prepare two arrays, one is input and hidden unit and the second is output unit.

Here first is a two dimensional array W_{ij} is used and output is a one dimensional array Y_i.

3. Original weights are random values put inside the arrays after that the output**.**

$$x_j = \sum_{i=0} y_i W_{ij}$$

Where, y_i is the activity level of the j^{th} unit in the previous layer and W_{ij} is the weightof the connection between the i^{th} and the j^{th} unit.

4. Next, action level of y_i is estimated by sigmoidal function of the total weighted input.

$$y_i = \left[\frac{e^x - e^{-x}}{e^x + e^{-x}}\right]$$

When event of the all output units have been determined, the network calculates the error (E)**.**

$$E = \frac{1}{2}\sum_i (y_i - d_i)^2$$

Where, y_i is the event level of the j^{th} unit in the top layer and d_i is the preferred output of the j_i unit.

Calculation of error for the back propagation algorithm is as follows:

- Error Derivative (EA_j) is the modification among the real and desired target:

$$EA_j = \frac{\partial E}{\partial y_j} = y_j - d_j$$

- Error Variations is total input received by an output changed

$$EI_j = \frac{\partial E}{\partial X_j} = \frac{\partial E}{\partial y_j} X \frac{dy_j}{dx_j} = EA_j\, y_j\,(1 - y_i)$$

- In Error Fluctuations calculation connection into output unit is required:

$$EW_{ij} = \frac{\partial E}{\partial W_{ij}} = \frac{\partial E}{\partial X_j} = \frac{\partial X_j}{\partial W_{ij}} = EI_j\, y_i$$

- Overall Influence of the error:

$$EA_i = \frac{\partial E}{\partial y_i} = \sum_j \frac{\partial E}{\partial x_j} X \frac{\partial x_j}{\partial y_i} = \sum_j EI_j W_{ij}$$

4. PROPOSED SYSTEM

This section describes the proposed network organization and server decision making methodology. Additionally this section contains simulation setup for simulating the network performance and effect of attacks in network performance.

4.1 Network Roles

The proposed system is a data mining based secure ad hoc infrastructure. In this proposed network system the network nodes are identified in three main roles. These roles in network are decided according to the computational ability and their positioning in network. Therefore the system consist of a intelligence server node which includes a trained neural network for decisional capability, cluster heads which works as intermediate node for collection of network samples and information. In addition of the client nodes who consume the network service, these three main kinds of devices and their responsibilities are discussed as.

Client Nodes: Clients are follows characteristics of MANET devices which are able to send, receive and route data in the network. During internal cluster communication and during external communication first cluster head check the validity of communicating node after that able to communicate with the external node.

Cluster head: These devices are working in two different operating modes. First linked connectivity all the cluster heads are connected through the server machine by a backbone network. Additionally able to collect data samples, send and receive data during the communication. And in second as Wi-Fi nodes which is directly in contact of mobile nodes.

Server Node: server node is implemented with an intelligence algorithm which works with data collected from the network source and analyses to get the behaviour of newly introduced nodes or making the detection and prevention of attack decisions.

In order to simulate the different nodes and their roles in network the figure 2 provides the simulation screen of the implemented scenario. In this diagram the red colour nodes shows the attacker nodes in network, blue nodes shows the end client nodes additionally the pink colour node and purple.

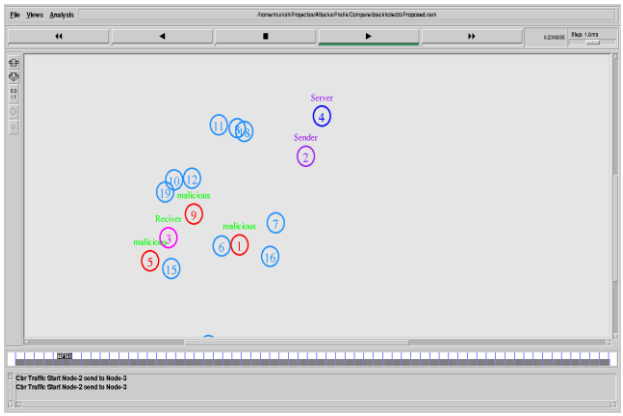

Figure 2 Neural Network

4.2 Decision Making

The entire processes between end client, cluster head and the decisional server is provided using figure 3. In this diagram secure communication based on the three defined roles is performed. Basically client node is a simple Wi-Fi node which performs communication as other mobile ad hoc devices are communicating. The cluster heads are fixed devices which collect the network traffic information. The traffic data includes remaining energy of nodes, round trip time from node and remaining buffer length.

For data collection, after a predefined time the data is collected using cluster heads and updated on server node. That can be understood by the following example. Suppose first traffic sample is collected at the time t_1 and after a defined time Δ, at time t_2 again sample is collected. Thus between time t_1 and t_2 required sample is estimated using the following formula.

Energy is computed as:

$$E_t = \sum_{i=1}^{N} \frac{E_t^1 - E_t^2}{t_1 - t_2}$$

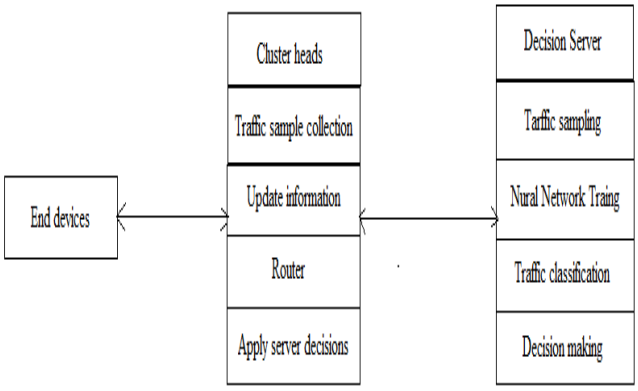

Figure 3 proposed network architecture

In the same way buffer size threshold values are computed

$$B_t = \sum_{i=1}^{N} \frac{B_i}{N}$$

For packet delivery ratio

$$PDR_t = \sum_{i=1}^{N} \frac{PDR_t^1 - PDR_t^2}{N}$$

And for constructing the RTT value the following formula is used.

$$RTT_t = \sum_{i=1}^{N} \frac{T_d - T_s}{2H}$$

The estimated data samples collected through concerning cluster head and the estimated values are updated on the server node as the server traffic sample. This traffic data is organized in server machine as given in table 2.

Table 2 Training set example

E_t	RTT_t	B_t	PDR_t	Behaviour

The table 2 includes additional attributes which contains the behavior of nodes. These behaviors are provided as input during training and after learning of the neural network incoming traffic is used for recognizing the malicious pattern from collected sample. The proposed data model is very effective and accurate for classifying patterns thus the model is able to differentiate the malicious and normal nodes. Now the server broadcast a cryptographic key to all the nodes that are legitimate in network. after the key distribution the source initiate the communication using the RREQ flooding after that when the receiver node send reply message then the receiver node send their key with RREP message. When the source node get the reply from the destination node then the source node extract the key included in RREP packet and compare it with the server generated key. If both the keys are similar than the source recognize the route is secured else that contains a malicious node. The entire process of the malicious node discovery can be understood by the following algorithm steps.

1. Initialize network with N nodes at time t_1
2. Wait for Δtime and after that at time t_2
3. Cluster heads calculate $E_t, B_t, RTT_t \; and \; PDR_t$
4. Update server node with calculated values
5. For each in coming traffic in server node
6. $classify\ (traffic\ data) = \begin{cases} 0 & if\ node\ malicious \\ 1 & if\ node\ ligitimat \end{cases}$
7. End for
8. Server generate Key
9. Broadcast key to all nodes that have legitimate values
10. Sender initiate route discovery using RREQ flooding
11. Receiver add server key with RREP message
12. Sender get the RREP
13. Extract receiver added key
14. If receiver key = = senders Key
15. Node is legitimate
16. Else
17. Node is malicious
18. Drop reply message
19. End if
20. Node is malicious
21. Drop reply message
22. End if

The implementation of the data model namely neural network is performed using the C++ technology and the implementation of all the network system is performed using the NS2 network simulator.

4.3 Simulation Setup

In order to simulate the effectiveness of the proposed attack analysis the following network parameters are setting up for network simulation.

Table 3 Simulation Scenario

Simulation properties	Values
Antenna model	Omni Antenna
Radio-propagation	Two Ray Ground
Channel Type	Wireless Channel
Network Interface	Phy/Wireless Phy
MAC	Mac/802_11
CBR Packet Size	512 Byte
Interface Queue Length	Queue/Droptail/PrioQueue
Dimension	750 X 550
No of Mobile Nodes	20, 40, 60, 80, 100
Routing protocol	AODV
Time of simulation	100 Sec.

4.4 Simulation Scenario

In order to characterize the effect of considered attacks the following scenarios are desired to implement with the simulation.

1. Simulation of black hole attack: in this scenario for demonstrating the effect of black hole attack a MANET configured using AODV routing protocol additional a network is configured using the proposed network system. After that a black hole node is deployed on both the network and their performance of the network is measured and compared.

2. Simulation of the wormhole attack: in the similar way in the simple network and proposed network is configuration with the wormhole link and the performance of the network is compared.

3. Simulation of grey-hole attack: in this scenario in MANET a gray-hole attack is deployed on the proposed network and normal network. Additionally the performance is computed and compared with the normal MANET.

4. Simulation of DDOS attack: in this scenario the DDOS attack is deployed in network and the performance of the network is estimated and compared with the normal network under attack conditions.

5. PROPOSED SYSTEM

After implementation of the proposed network infrastructure the mobile ad hoc network is configured and simulated using NS2 simulator. After simulation using the generated trace files the performance of the network under different attack conditions are evaluated and compared. For experimentation and effective performance investigation the number of node during simulations are increases and the experimental results are organized in this section.

5.1 Packet Delivery Ratio

The packet delivery ratio is an amount of packets which are successfully delivered on the target machine. That can be estimated using the following formula.

$$Packet\ delivery\ ratio = \frac{total\ delivered\ packets}{total\ sent\ packets}$$

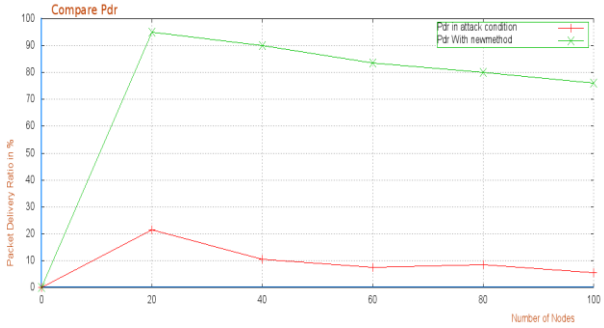

Figure 3 PDR during DDOS Attack

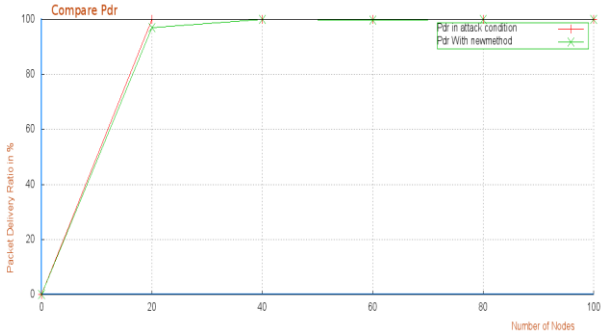

Figure 4 PDR during DDOS Attack

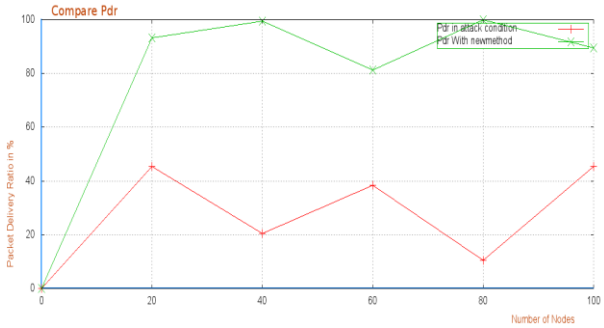

Figure 5 PDR during Gray Hole Attack

The performance of the network (proposed and normal MANET) in terms of packet delivery ratio is given using figure 3, 4, 5 and 6.In both of the network a black hole node is deployed and the performance the performance of both the networks is estimated as given figure 3. In this diagram the performance of the proposed network is given using green line and the performance of network is given using red line. According to the results during black hole attack the traditional network performance is gone below and the proposed network is not affected. In the similar way the performance of the network under DDOS attack is given using figure 4, under the gray whole attack is given using figure 5 and under wormhole attack is simulated using figure 6. In all the simulation the performance under the attacks in normal network significantly reduces the packet delivery ratio on the other hand the in proposed network the performance in terms of packet delivery ratio is not affected.

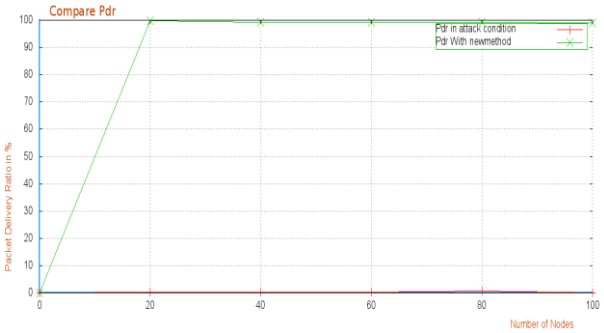

Figure 6 PDR during Wormhole Attack

5.2 Remaining Energy

The network nodes are built with the limited energy resources thus for each events in network node the node consume a fixed amount of energy. The remaining and comparative energy during different attacks conditions namely black hole, DDOS, gray hole and wormhole attack are simulated using figure 7, 8,9 and 10 respectively .According to the obtained results the energy consumption of nodes are reduces in case of the proposed network configuration. On the other hand the node energy during different attacks in normal mobile ad hoc network is drained frequently. For simulating the network performance of both the networks the red line represents the energy drop of normal network and the green line shows the energy drop during the proposed algorithm implementation. According to the obtained results the proposed network intrusion detection technique is effective and reduces the power consumption and optimizes the resource consumption too even the network having the malicious behaving node.

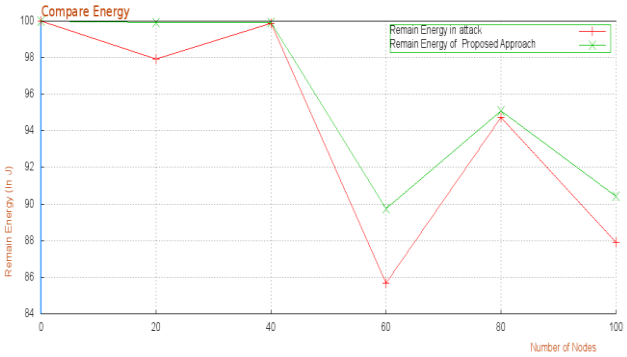

Figure 7 Energy during black hole attack

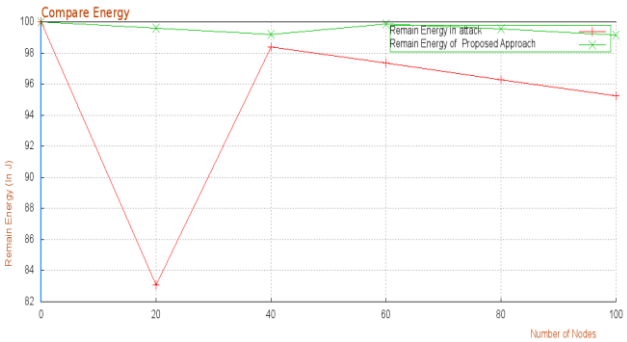

Figure 8 Energy during DDOS attack

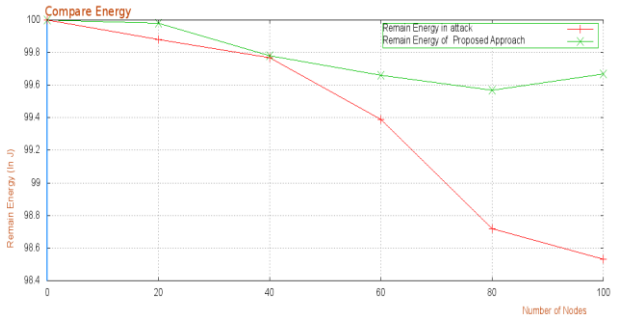

Figure 9 Energy during gray hole attack

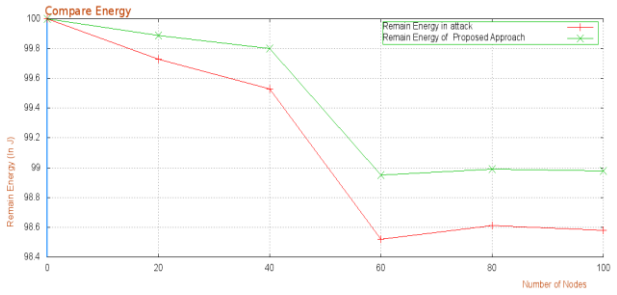

Figure 10 Energy during wormhole attack

5.3 End to End Delay

End to end day on network refers to the time taken for a packet to be transmitted across a network from source to destination device, this delay is calculated using the below given formula.

E2edelay = receiving time – sending time

The comparative network performance in terms of end to end delay is given evaluated. During the black hole node deployment the e2e delay is given using figure 11, during DOS attack is given using figure 12, during gray hole given using 13 and during wormhole given using figure 14.

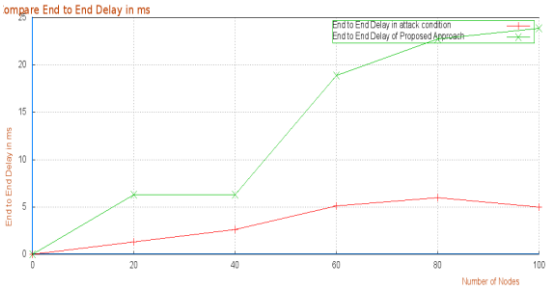

Figure 11 e2e during black hole

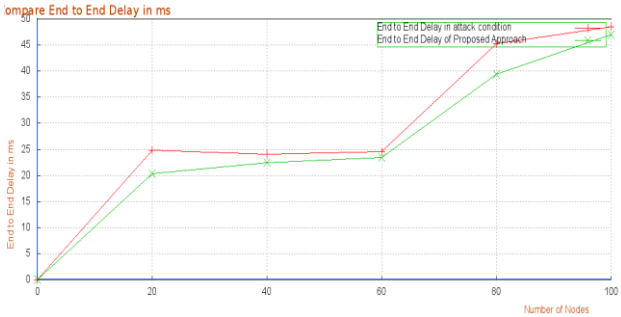

Figure 12 e2e during black hole

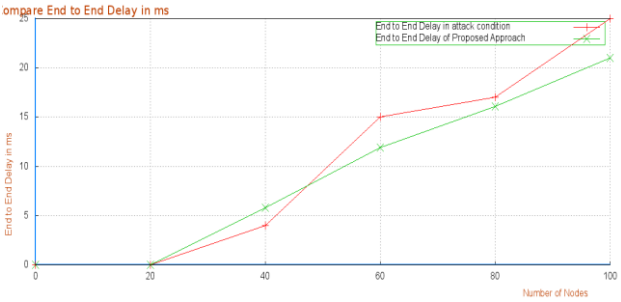

Figure 13 e2e during black hole

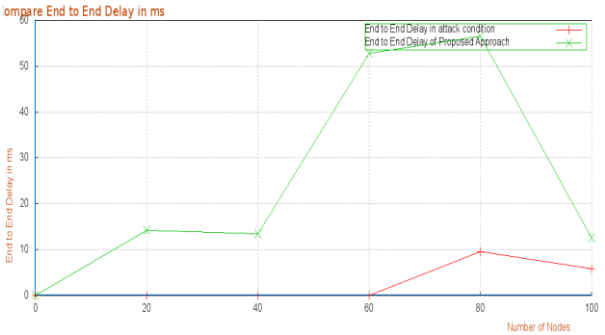

Figure 14 e2e during black hole

According to the simulated performance the normal network performance in terms of end to end delay is simulated using red line and the proposed network is simulated green line. The results show the proposed network organization is much robust during different attacks conditions.

5.4 Routing Overhead

The amount of additional packets injected on network during the communication sessions is known as the routing overhead.This section describes the routing over head during different attacks on traditional mobile ad hoc network and proposed network infrastructure. For simulating performance the proposed method is given using green line and the performance of traditional technique is given using red line. During the black hole and DDOS attack the end to end delay in network is increase exponentially on the other hand the attack not affect the performance in proposed methodology. Additionally in case of the grayhole attack and wormhole attack the performance of the proposed network is also affected in terms of end to end delay. But in less dense network conditions it is able to classify the traffic more accurately. Therefore during nodes 20 and 40 the performance of network is adoptable and the performance of network is affected when node density exceeded.

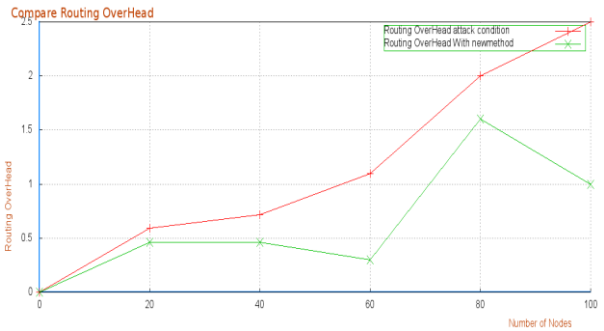

Figure 16 routing overhead during black hole

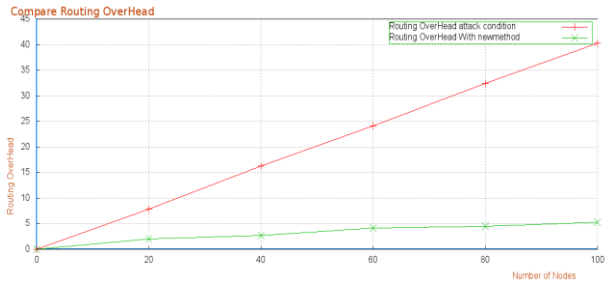

Figure 17 Routing overhead during DDOS

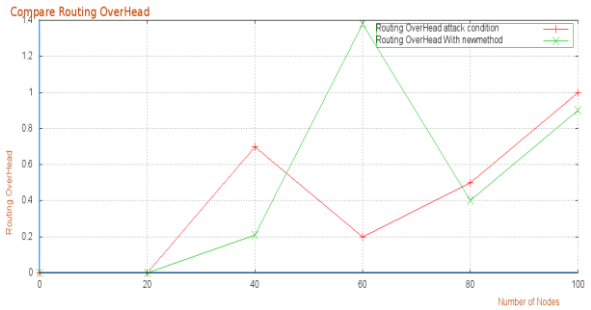

Figure 18 Routing overhead during gray hole

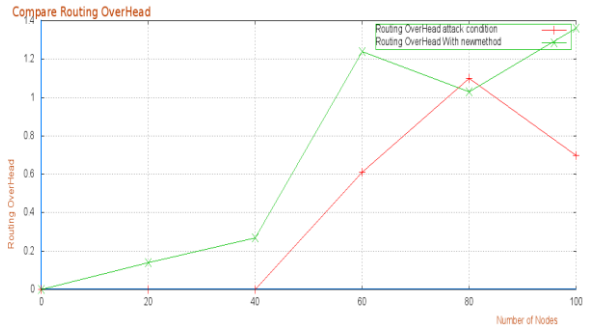

Figure 19 routing overhead during wormhole

5.5 Throughput

Network throughput is the usual rate of successful delivery of a message over a communication medium. This data may be transmit over a physical or logical link, or pass by a certain network node. The throughput is calculated in terms of bit/s or bps, and occasionally in terms of data packets per time slot or data packets per second. The performance of the proposed and traditional technique is compared and for representation red line for traditional MANET and for proposed green line is used. According to the observation of results in normal MANET during different attacks the throughput is decreases significantly on the other hand the performance of network in proposed network is not affected from attack.

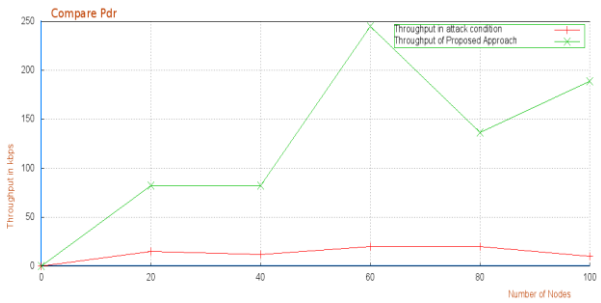

Figure 20 Throughput during black hole

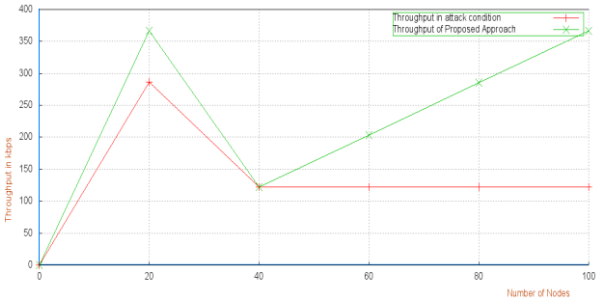

Figure 21 Throughputs during DDOS

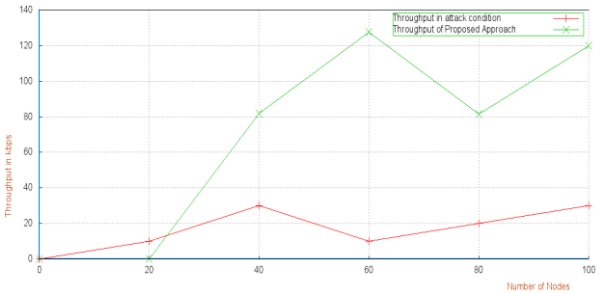

Figure 22 Throughput during gray hole

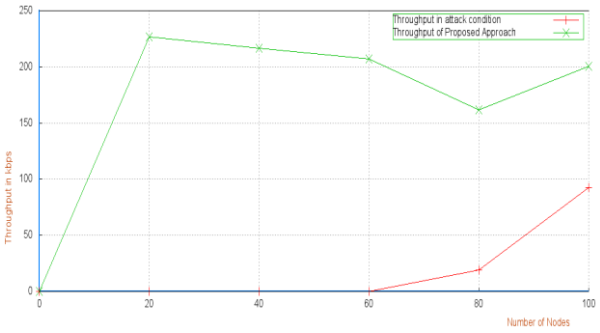

Figure 23 Throughput during wormhole

In this section the performance evaluation and results analysis is performed. The entire research summary is given in next section additionally the future extension of the presented methodology is provided.

6. CONCLUSION AND FUTURE WORK

The proposed work is intended to find solution for the mobile ad hoc network security. Therefore a number of techniques are explored first for finding the network and attacker's characteristics. Than after various machine learning techniques are investigated for finding the accurate pattern identification.

Finally for detecting attacks in network a machine learning based intrusion detection system is implemented and simulated. The proposed MANET IDS system includes the new network configuration and attack detection technique additionally using the traffic samples classification. For accurate classification the back propagation neural network is used.

The implementation of the proposed concept is provided using the the NS2 and C++ scripts. After implementation of the system the performance of the proposed system is evaluated in terms of end to end delay, routing overhead, remaining energy, packet delivery ratio and throughput. Results shows the effective performance of the system even when the network contains the attackers.

In near future the system is enhanced more for finding more kind of attacks in network by including more parameters in proposed attack detection technique.

7. REFERENCES

[1] Kshmeera N. Khachar and Mrs. Jayna B. Shah, "Detection and Prevention of Black hole Attack in Mobile Ad-hoc Networks: A Survey", IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, P-ISSN: 2278-8727, Vol. 26, Issue 2, Ver. XI (May-April 2014), PP. 108-112.

[2] Martin K Parmar, Harikrishna B Jethva, "Survey on Mobile ADHOC Network and Security Attacks on Network Layer", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013.

[3] Meghna Chabra and B.B. Gupta, "AN Efficient Scheme to Prevent DDos Flooding Attacks in Mobile Ad-hoc Network (MANET)", Research Journal of Applied Sciences, Engineering and Technology 7 (10): 2033-2039, 2014, ISSN: 2240-7459; e-ISSN: 2040-7467, PP. 2033-2039, © Maxwell Scientific Organization, 2014.

[4] Asma Tuteja, Rajneesh Gujral, Sunil Thalia, "Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2", 2010 International Conference on Advances in Computer Engineering, 978-0-7695-4058-0/10 $26.00 © 2010 IEEE.

[5] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamurlidhar, " A Mechanism for Detection of Grayhole Attack in Mobile Ad-hoc Networks", ICICS 2007, 1-4244-0983-7/07/$25.00*©2007 IEEE.*

[6] XiaoHang Yao, "A Network Intrusion Detection Approach Combined with Genetic Algorithm and Back Propagation Neural Network", 2010 International Conference on E-Health Networking, Digital Ecosystem and Technologies, PP. 402-405, 978-1-4244-5517-1/10/$26.00©2010 IEEE.

[7] Abhinav Jain, Sanjay Sharma and Mahendra Singh Sisodiya, "Network Intrusion Detection by using Supervised and Unsupervised Machine Learning Technique: A Survey", International Journal of Computer Technology and Electronics Engineering (IJCTEE), PP. 14-20, ISSN 2249-6343, Volume 1, Issue3.

[8] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, March 2013

[9] Martin K Parmar, Harikrishna B Jethva, "Survey on Mobile ADHOC Network and Security Attacks on Network Layer", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013.

[10] Context-Sensitive and Adaptive Routing in Wireless Mobile Ad-Hoc Networks Using Cross-Layer Design, http://www.uni-marburg.de/fb12/verteilte_systeme/ forschung/pastproj/adhoc_routing_emul

[11] AsmaTuteja, Rajneesh Gujral, Sunil Thalia, "Comparative Performance Analysis of DSDV, AODVand DSR Routing Protocols in MANET using NS2",2010 International Conference on Advances in Computer Engineering,978-0-7695-4058-0/10 $26.00 © 2010 IEEE.

[12] R. Bronson and G. Naadimuthu, "Operations Research", 2 ed., Schaum's Outlines, McGraw Hill, New York, 1997.

[13] Atul Patel, Ruchi Kansara, Dr. Paresh Virparia, "A Novel Architecture for Intrusion Detection in Mobile Ad-hoc Network", International Journal of Advanced Computer Science and Applications", PP. 68-71, Special Issue on Wireless and Mobile Ad-hoc Networks.

[14] CH.V. Raghvendram, G. Naga Satish and P. Suresh Varma, "Security Challenges and Attack in Mobile Ad-HOC Networks", I.J. Information Engineering and Electronics Business, 2013, 3, PP. 49-58.

[15] Weichao Wang, Bharat Bhargava, Yi Lu and Xiaoxin Wu, "Defending Against Wormhole Attacks in Mobile Ad-hoc Networks", Wiley Journal of Wireless Communication and Mobile Computing (WCMC), PP. 1-24.

[16] Ochola EO and Eloff MM, "A Review of Black Hole Attack on AODV Routing in MANET, Marsan, M.A. (2001): Optimal multicast scheduling in input-queued switches, Proc. IEEE Communications, pp. 2021-2027.

[17] J. Ryan, M. Lin and R. Miikkulainen, Intrusion detection with neural networks. AI approaches to fraud detection and risk management: papers from the 1997 AAAI workshop (Providence, Rhode Island), PP. 72-79.

[18] Z.M. Yang et al., "An intrusion detection system based on RBF neural network", Proceedings of the Ninth International Conference on Computer Supported Cooperative Work in Design, 2005. Vo1.2, 2005, cscwd, PP. 873-875.

[19] J. Zhong, Z.O. Li et al., Intrusion Detection Based on Adaptive RBF Neural Network. Proceedings of the Sixth International Conference on Intelligent Systems Design and Applications (ISDA'06) - Volume 02, 2006, PP. 1081- 1084.

[20] Z.J. Tang et al., Intrusion Detection. Tsinghua University Press, 2004, Chap.2, PP. 6-8.

[21] P. Innella P, O. McMillan, An introduction to intrusion detection systems. Tetrad Digital Integrity, LLC, last updated December 6, 2001, http://www.ecurityfocus.comlinfocus/ 1520.

[22] C. Stergiou, D. Siganos, Neural Networks. http://www.doc.ic.ac. ukI-ndisurprise 96/journal/vol41 cs 1 1/report.html.

[23] Vikas Makram and Shirish Mohan Dubey, "A General Study of Associations rule mining in Intrusion Detection System", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 1, January 2012.

[24] Qinglei Zhang and Wenying Feng, "Network Intrusion Detection by Support Vector and Ant Colony", In: Proc. of 2009 Intl. workshop on information security and applications (IWISA 2009).

[25] Ashan Ozkaya and Bekir Karlık, "Protocol Type Based Intrusion Detection Using RBF Neural Network" International Journal of Artificial Intelligence and Expert Systems (IJAE), Volume (3): Issue (4), 2012.