Detection and Prevention of Manet using Hybrid SVM with Ann

Vishal Walia, Rahul Malhotra

Abstract*: Mobile Ad hoc Networks (MANET) have been exceptionally vulnerable against attacks because of the dynamic and self-configurable nature of its system foundation. This kind of wireless network is appropriate for temporary communication linked due to its nature of less-foundation and there is no any control of centralized manner. Design a routing mechanism that are security aware with higher QoS parameter is very competetive and the major tasks involved in ad hoc types of network as per the limited power resources and their dynamic routing topology. This paper mainly focused on the design of a secure and trusts based on-demand routing mechanism using Ad-hoc on demand distance vector (AODV) protocol to compute trust-based produces path initialed from source up to destination that will fulfill minimum two end-to-end QoS parameters of network. So here, the generalized AODV routing protocol has been extended from traditional routing mechanism to analyze the performance of this model with combination of artificial intelligence concept. The proposed ad hoc based routing mechanism is used to found possible routes that are prevented through trust adjacent position of security validation protocols and enhanced link optimized route computes on the basis of Artificial Neural Network (ANN) as an artificial intelligence algorithm for well-organized communication in MANET. In addition, this research demonstrates the effectiveness of bio inspired Firefly Algorithm (FFA) as an optimization approach with the consideration of several performance QoS metrics of network. The results have been measured in terms of throughput and PDR with SVM and ANN approach. It has been observed that the throughput and PDR measured using ANN approach is better compared to SVM approach an average of 0.755 PDR value has been obtained using ANN approach.

Keywords*: Mobile Ad hoc Networks, d-hoc on demand distance vector, Artificial Neural Network, Firefly Algorithm, SVM, and PDR.

I. INTRODUCTION

MANET (Mobile Ad hoc Network) is defined as a set of autonomous users who communicate in a relatively limited bandwidth area. These networks are considered mobile nodes that are moving without base station [1]. Therefore, the communication process is control by these nodes itself. For data transmission routing plays a very important role in MANET[2,3]. Routing is a mechanism for transferring data directly from source to communication network. The main reason is that previous networks are manageable and have an integrated environment; at the same time, a high-volume and large-scale network is the latest development in telecommunications networks and technology [4,5]. The basic operation of routing mechanism is to perform two tasks: first, finding the optimal route, and second, sending data groups known as packets over the network [6]. Also to optimize the route Firefly algorithm is used and the selection has been performed using ANN approach.

Revised Manuscript Received on December 30, 2019.

* Correspondence Author
Vishal Walia*, PHD Scholar IGKPTU, Jalandhar, India .vishal.walia4p@gmail.com
Dr. Rahul Malhotra, Director , Guru Teg Bahadur Khalsa Institute of Engineering & Technology, Chhapianwali, Malout, India

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

II. RELATED WORK

The attack of kind black hole is a major issue and by utilizing the trust-factor, the system becomes reliable. For each and every node, a model based on trust is built inside the area of network. This presented system has implemented for IDS (Intrusion Detection system) to identify and mitigate MANET black-hole attacks. N. Arya et al. [7] prevented the network from attacks makes more secure. It facilitates the enhancement of the PDR and reduces overhead control by improving the performance of the routing protocol. The future lies in improving the table entries in the destination node for more effective detection of wormhole nodes. here, network security by using effective techniques to prevent hybrid has also provided and improved DoS attacks by the help of a novel algorithm. P. Gupta et al. [8] used the network in every field and the power of the clients assured about the growth of MANET. MANET is defined like a distributed system that do not requires a certain transmission network or backend since it executes user connections with the available nodes. A number of executions were carried out in MANET, ranging from defense to multi-user gaming, which requires the network to be saved from various attacks and trespassers. The researchers used the ECBDS to store the network from the particular attack namely Byzantine attacks and the use of resources. T. A. Kolade [9] haveimplemented a system having mobile network operates taken as a node and is termed as less-infrastructure and wireless network having nodes are moves in free manner and positions can also be varies . The resources utilization has been detected on the basis of a new algorithm for security level. The bandwidth utilization and storage for few node never depend up on the threshold configuration being used properly. The attack named as Byzantine has been observed if the accused is not regarded in due time through some sources. A. Adnan et al. [10] have utilized various kinds of loads and simulation measurements.

As a result, QoS metrics named as; PDR, Throughput and AE2ED are tested in the network being deployed.

The generated outcomes after the simulation showed that the performance of the network in black hole attacks has been decreased predominantly in PDR due to the nodes discarding each of the data packets traversing the path. In fact, throughput efficiency has significantly decreased in the life of malicious nodes. This can be happened due to the reason of the lack of distribution to the recipient of the packets getting transferred. If there is no any effect of black hole attack, there is some amount of increment in the AE2ED. It has to be acknowledged as suspicious nodes, before confirming about the routing table, immediately transmitted the response. In the QoS parameters some variations have been occurred that can be showed the performance of network, mainly decreased in the presence of a black hole attack. Jain et al. [11] have explored a network using fuzzy based model. The model has been utilized for the detection of black hole attack through consuming AODV along with Fuzzy based approach. The entire process has been performed using NS-2 simulator by deploying 50 numbers of nodes that are moving in the area about 1km. The network has been used to detect malicious nodes up to 2 to 80 %, which is possible by employed fuzzy logic as a classification approach. Chhabra et al. [12] have implemented a approach based on fuzzy potential Threat protocol to protect MANET from Black hole attack. The designed protocol has helped to deliver data on time with smaller packet drop. The main problem that has been find out in this research is that the nodes taken decision as per the rank list. This result in increase in storage modules included with decreases the communication speed. Abdel-Azim et al. [13] have presented a scheme to utilized Genetic algorithm as an optimization approach with Fuzzy and Neural network to minimize the influence of black hole attack in MANET. According to the obtained result it has been observed that the rate for packet delivery after getting the network secure from black hole attack is less compared to the Intrusion Detection System (IDS) used in the network. From the literature it has been studied that, to prevent MANETs becomes a necessary to their deployment and use as MANET is used in vast secure areas where data security and interaction are essential. Established wireless network methods have used to achieve some degree of security. However, such kinds of options may always be adequate; as the ad hoc network has its own security issues due to these solutions can not be resolved. In such a scenario, a protection solution should always be combined with such an intrusion detection system to achieve an appropriate degree of security. A comprehensive approach for detecting intrusion included in mobile nodes of MANETs has proposed. This system in based on behavioral-anomaly, that makes it flexible, scalable, customizable, and reliable. ITuse AN AODV routing protocol to verify our system by running mobile node simulations. It is very difficult to build an intrusion detection system for wireless ad hoc networks. Wireless network's very existence, i.e. lack of fixed infrastructure, makes it difficult for the network to obtain audit information. The wireless network's limited resources are critical parameters to be considered when developing the Black Hole Attack Secure Framework. Many times make a distinction in between the false alarms and a true positive is very difficult task. The SVM technique is taken to resolve this issue.

III. PROPOSED WORK

The model of proposed work has categorized among two sections: Route Discovery and its improvement, detection and mitigation of threats. Initially a network using n number of nodes is deployed using coordinate geometry to position the nodes within the network. The design process of network creation is described below.

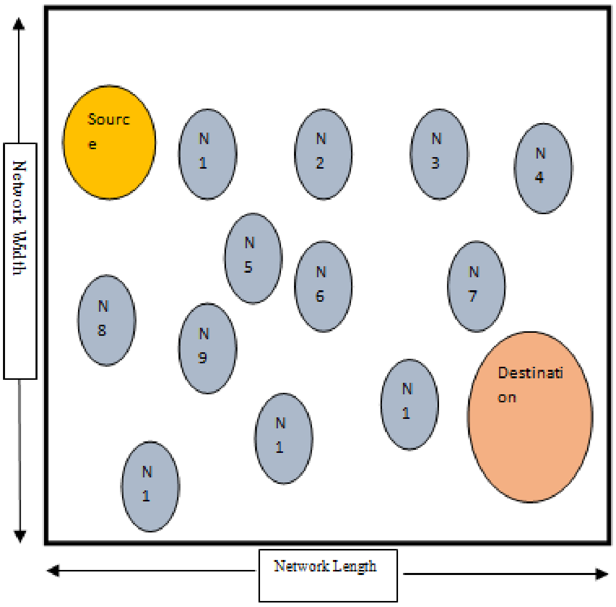


Fig. 1 Create network

The designed ad hoc network with 12 numbers of nodes along with one source and one destination nodes are displayed in Fig. 2. The source and the destination servers are represented by the yellow and the pink color respectively.

IV. MATH

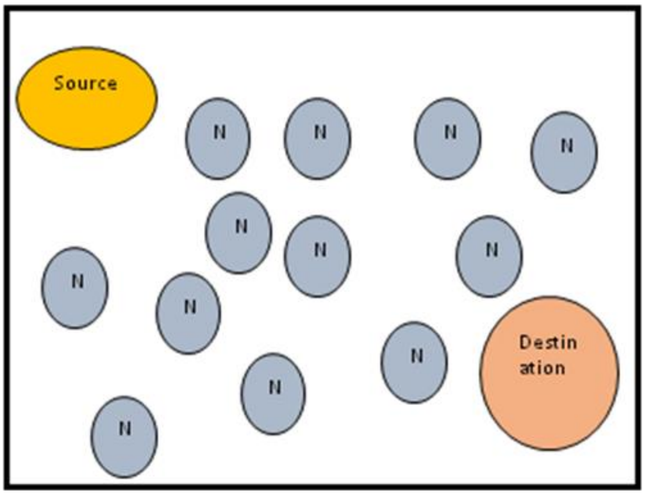


Fig. 2 Route Formation

After nodes deployment next step is to find route in between the source and, the destination server. The route is formed by applying AODV as a route creation mechanism. The process of finding route is discussed below.

A. Route Discovery

To discover a route, AODV is used as a routing protocol. This is a reactive routing protocol, in which route is formed only when the nodes required to transmit data. It works mainly into two predefined phases: (i) Route request and (ii) Route Discovery. Initially, Route request is sent by the transmitting node throughout its coverage range in the MANET. When the route request packet is received by the nearby node, it stores the address in its route list table. If the address is not matched with the nearby node, then it forwards the request packet to its nearby node and an acknowledgement in terms of reply packet send to the transmitter node that means current node is not a destination. In this way, the packet reached at its destination node through multiple possible routes.

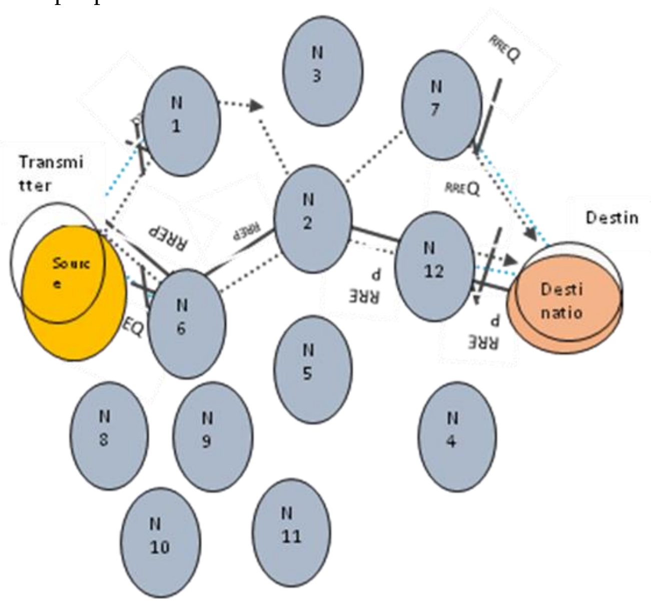


Fig. 3 Route Discovery Process using (AODV)

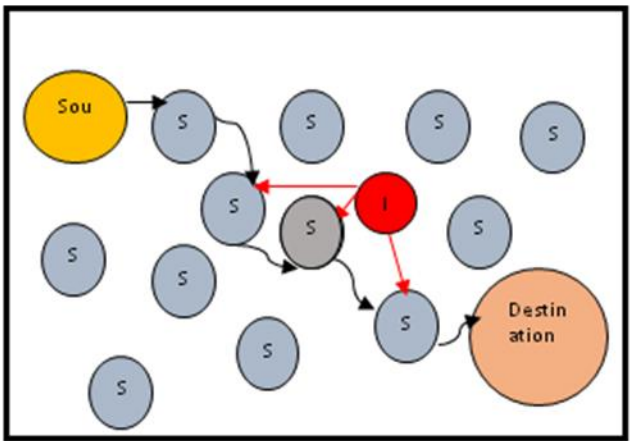


Fig. 4 Affected Node

The attacker (black hole /gray hole) starts dropping data packet and hence decreases the throughput. The affected node is represented by gray color as depicted in Fig. 4. To overcome this problem ANN along with SVM is used and the route is diverse through the node, N11. In this way the network is protected from the attacker. The proposed model uses the power consumption of respondents and their network operation time as the key source of light. It also determines the light level by taking into account the lighting time. Any respondent who meets the flying threshold shall be selected and the less difference value should be selected as the respondent.

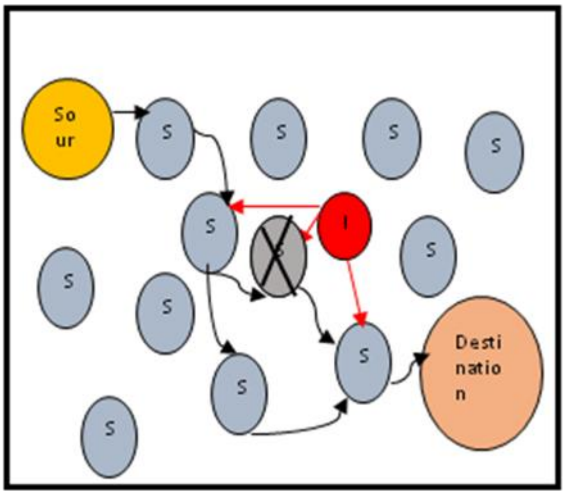
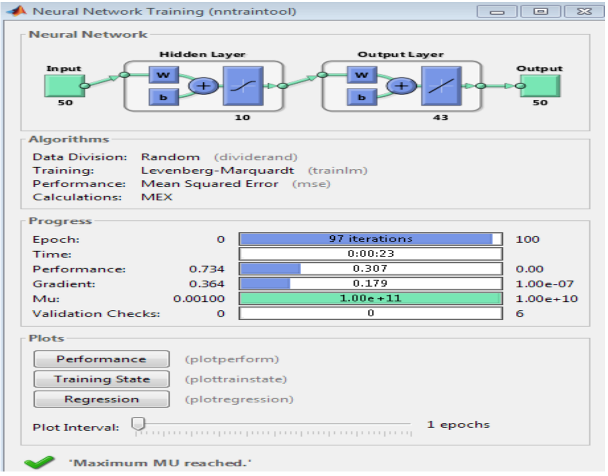


Fig. 5 Prevented Network

SVM has considered to be that path along included its related consumption of energy and the delay in the path as the proposed design stored a records of every path and node. Therefore it becomes a supervised learning process; the classified route would be the similar as the practice route transferred. In this particular case, if the element of the path does not suit for the pointed element, it can be called a suspicious route. The same design is used and listed for each path. The only difference is that the power consumption for the path is replaced by the node's power consumption and the delay generated by the path is replaced by the delay created through individual nodes.

B. USE OF ANN

In this research, three layer architecture of ANN is utilized for classification of the attack named as black hole by using the concept of deep learning tool box of MATLAB. Following is the input data, which is provided in the structure of input layer of ANN. The input data has been forwarded to the hidden layer in which the processing of data has been performed. In case of unwanted results, the error, which is termed as Mean Square Error (MSE) signal is feedback to the hidden layer. Based on the input values, the network is trained and later on used to detect black hole attack in the network. The training structure obtained after the training process is shown in Fig. 6.



Algorithms
Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MEX

Progress

Epoch:	0	97 iterations	100
Time:		0:00:23	
Performance:	0.734	0.307	0.00
Gradient:	0.364	0.179	1.00e-07
Mu:	0.00100	1.00e+11	1.00e+10
Validation Checks:	0	0	6

Plots
Performance (plotperform)
Training State (plottrainstate)
Regression (plotregression)
Plot Interval: 1 epochs

✓ 'Maximum MU reached.'

Fig. 6 Training Structure of ANN

Total number of nodes deployed inside the network is 50, and the properties have been given as input data of ANN. 10 number of neuron are passed to the hidden layer to adjust the weights according to the requirement and output in terms of 43 number of output data that represents the class of communicating nodes.

The SVM and ANN is utilized in the detection of nodes of black hole and gray hole in route using their optimized properties by Firefly. Initially, SVM is utilized for the detection of malicious node, after that validation has been performed using ANN approach. The algorithm of SVM with ANN is written below;

Algorithm: Support Vector Machine based Artificial Neural Network

Input: Optimized Properties of nodes (T), Types of node (Cat), Kernel Function, and Neurons (N)
Output: Authorized Nodes

```
Training:
1 Initialize the SVM training data T is the total nodes property with RBF as Kernel function
2 for I = 1→ All nodes
3     if Property of Node (I) == Real
4         Defined the Cat as a category of training data
5         Cat (1) = Nodes (I)
6     else
7         Cat (2) = Nodes (I)
8     end
9 end
10 Train_Structure=SVMTRAIN (T, Cat, Kernel function)
11 T= Train_Structure. SupportVector //To find out the training data for ANN
12 Initialize the basic parameters of ANN
        – Number of Epochs (E) // Iterations used by ANN
        – Number of neurons (N)
        – Performance: Mutation, MSE, Gradient and Validation
        –Techniques to be utilized: Levenberg Marquardt
        – Division of data: Randomly
13 for i = 1 → T
14     If T belongs to real nodes property
15         Group (1) = Properties of training data according to the real nodes
16     else if T belongs to non real nodes property
17         Group (2) = Properties of training data according to the non real nodes
18     else
19         Group (3) = Extra properties of training data
20     end
21 end
22 Initialization of ANN through Training data and then group them
23 Net = Newff ($T, Group, N$)
24 The parameters for training are set on the basis of the requirements and perform training
25 Net = Train (Net, data for training and, Group)
Testing:
26 Current Node = Properties of the current node in the network
27 Authorization = simulate (Net, Current node)
28 if Authorization is valid
29 Authorized node = Right
30 else
31 Authorized node = Wrong
32 end
33 Return; Authorized nodes as output
34 end
```

V. RESULTS AND ANALYSIS

As per the structure of classification, some parameters are analyzed.

a) Throughput : This parameter is computed as total amount of Received Packets per unit time
b) True Detection Rate(TDR) : It defined as the total true detected intruders divided by Total amount of detections
c) Packet Delivery Ratio(PDR) : It can be defined as the total number of packets that are received divided by total amount of transferred packets

The experimental result section is categorized into two sections (i) Results with SVM approach and (ii) Results with ANN approach

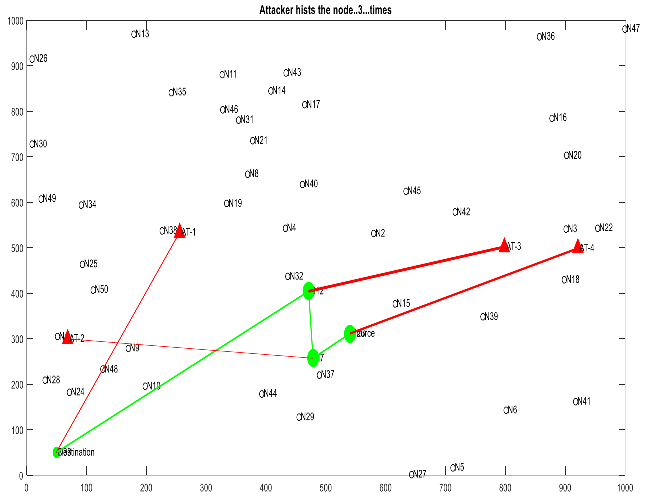


Fig. 7 Designed MANET Area

Initially MANET area of 1000 m^2 is designed by deploying 50 nodes in MATLAB as depicted in Fig. 7. It is observed that at the present network is attacked by 4 attackers represented by red triangles preventing the data transmission over the nodes represented by green spheres.

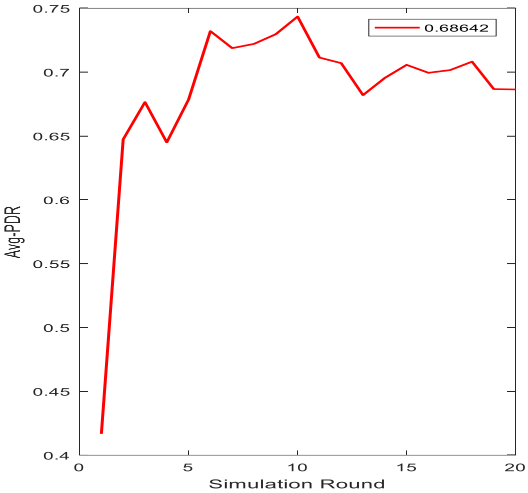


Fig. 8 Average-PDR performance

The PDR determines the actual data packets delivered over the network. Fig. 8 depicts the average PDR performance of the MANET over 20 different simulation rounds. It is observed that initially the average PDR rises steeply to a value corresponding to 0.654 for the first 3 simulation rounds. After this point, it rises from 0.65 to 0.675 with multiple fluctuations for the next 4 to 20 simulation rounds with an overall average PDR of 0.6862 attained for the 20 simulations.

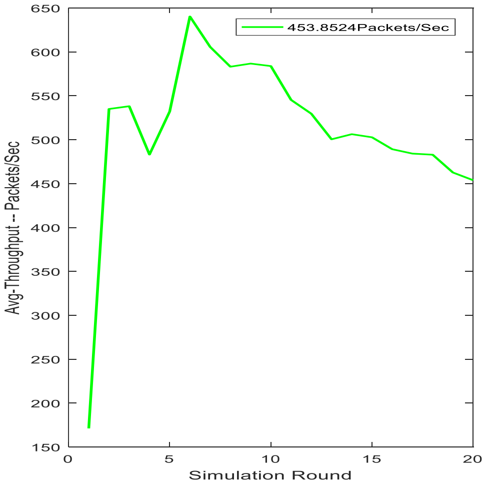


Fig. 9 Average-Throughput Variation

The average throughput variation of 20 simulations is shown in Fig. 9. The above Fig. corresponds to a steep rise of 540 packets per sec for the first 3 simulations. Later, throughput of the network reaches a peak value of 640 packets per sec at 6th simulation. Following this point, it gradually decreases to 458 packets/sec till the end of 20th simulation round. An overall average throughput of 453.8524 packets/sec is attained by the system over the 20 simulation rounds.

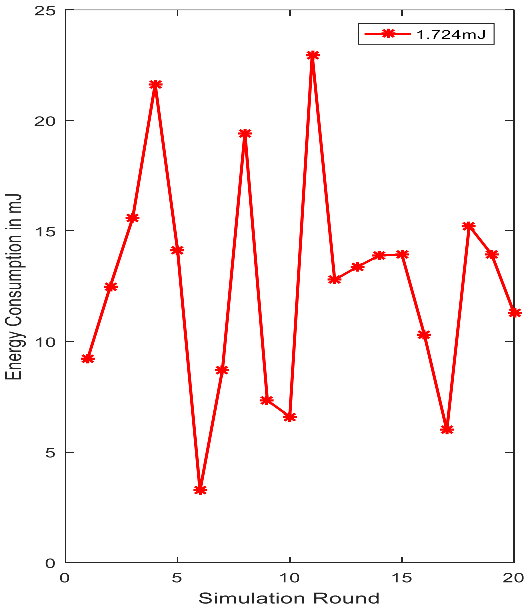


Fig. 10 Energy Consumption

Energy consumption by the system for 20 simulations is plotted in Fig. 10. The plot corresponds to multiple rise and fall in the magnitude of energy consumption by the system during simulations starting at 9mJ for 1st simulation round and ending at 11mJ for the last simulation round. It is observed that the system energy consumption ranges from 4mJ to 23mJ.

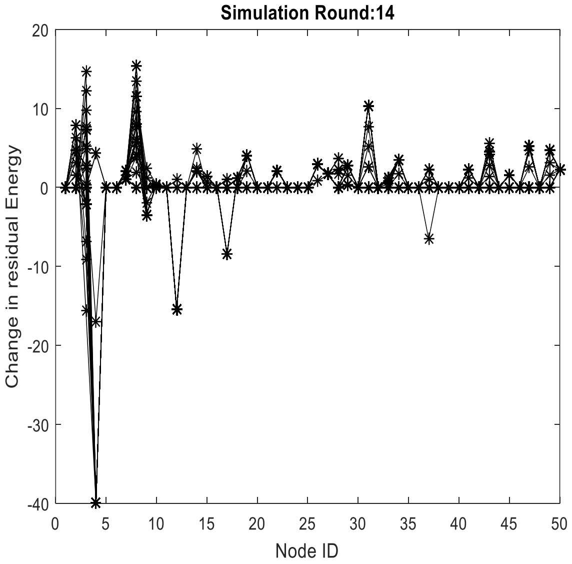


Fig. 11 Residual Energy Changes

Fig. 11 depicts the changes in the residual energy corresponding to 14th simulation round over 50 nodes considered in the study. The plot shows that on average residual energy of the system remains close to zero. Comparative analysis of Average network throughput using SVM and ANN is done based on three criteria, namely, normal, under threat and after prevention.

Table 1 summarizes the average throughput obtained for the said cases for both SVM and ANN for simulation rounds ranging from 100 to 500. It is observed that average throughput obtained for ANN is higher than SVM for all the three criteria.

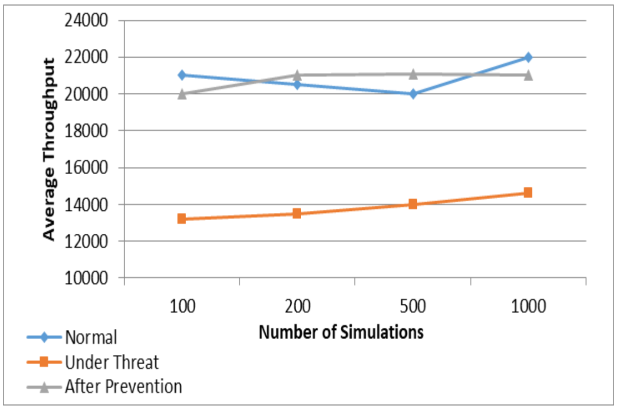


Fig. 12 Average throughput improvement using SVM

Fig. 12 compares the average throughput of the network under three circumstances namely the network acting normal in the network, the network under a threat and the network after the prevention using SVM. It has to be seen that the networks average throughput under the normal architecture is around 20875 data packets/ time frame. The measurable metrics of this work named as throughput lowers down when the system falls under threat. The throughput lowers down to about 13825 packets per second which is a downgrade by 33.77%. When the prevention algorithm is applied it goes nearly normal to around 20775 packets per time frame accounting to 33.45% improvement over the network under threat. It is obvious that, if you prevent anything, you could only attain what was the most normal, beyond that is not attainable.

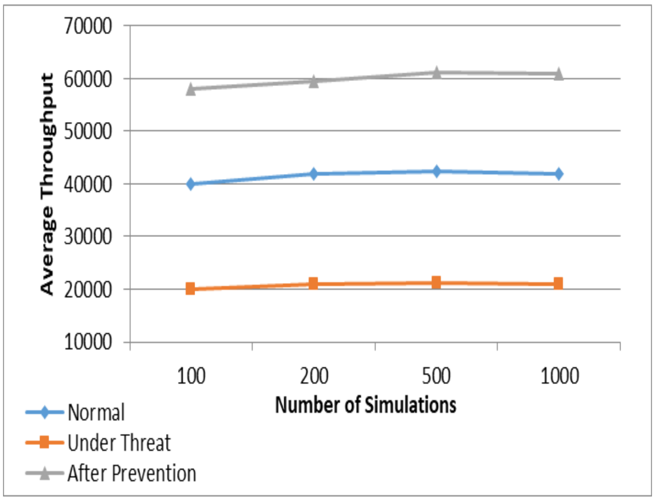


Fig. 13 Average throughput improvement using ANN

Average throughput obtained with ANN under three conditions is plotted in Fig. 13. It is observed that under normal conditions average throughput of network is 41625 packets per time frame that get lowered to 20775 packets per time frame under threat condition that corresponds to 50% reduction. The application of prevention algorithm re-establishes the network throughput to 59913 packets per time frame that corresponds to 65.32% improvement against the network under threat. It is observed that the throughput obtained using ANN approach is higher as compared to normal and under threat network.

PDR Evaluation

PDR evaluation is also done for normal network, network under threat and network after prevention using SVM and ANN. The resultant values of PDR under different conditions are listed in Table 2 for 100 to 500 simulations.

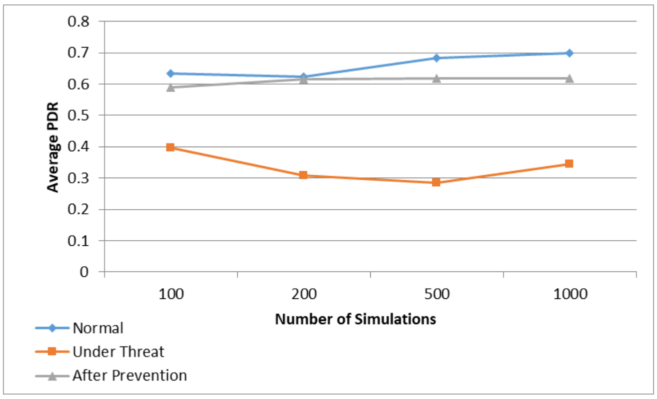


Fig. 14 Average PDR improvement using SVM

PDR evaluation under three conditions using SVM is plotted in Fig. 14. It is observed that average PDR of the normal structure is about 0.6603 which reduces to 0.3336 when it falls under the threat. The improvements are attained due to the dual phase threat discovery process followed by the route advancement architecture.

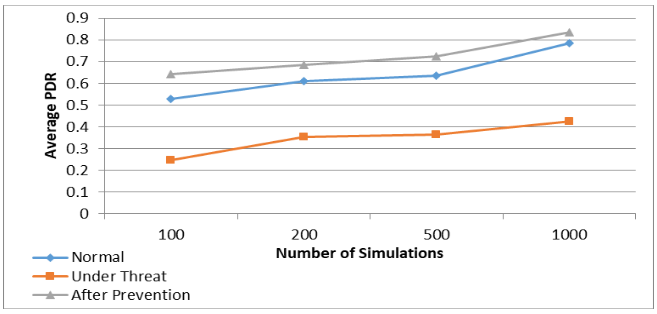


Fig. 15 Average PDR improvement using ANN

Fig. 15 represents the average PDR obtained for three scenarios, namely, under normal, under threat and improved after prevention using ANN as a classification approach. It is observed that PDR for the designed network under normal conditions is 0.6392 which get lowered by 45.61% under threat condition corresponding to 0.3476. Application of prevention algorithm increases the PDR to 0.7214 that shows that ANN delivered data has higher packet rate as compared to the packet rate obtained under threat condition.

VI. CONCLUSION

In the present work, routing mechanism for secure data transfer is presented for MANET that is susceptible to attacks. Simulation study is conducted for 500 rounds to parameterize the energy consumption, residual energy, throughput and PDR changes accompanying data transfer over the network.

Retrieval Number: B3537129219/2019©BEIESP
DOI: 10.35940/ijeat.B3537.129219
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The network effectiveness is evaluated for data transfer using PDR and throughput calculations under various conditions, mainly, data transfer efficiency over network under normal conditions is evaluated against the data transfer efficiency under attack and improved data transfer efficiency using SVM and ANN classification approaches to reach a well organized communication system. It is observed that throughput of the normal network get improved by 33.45% and 65.32% with the application prevention with SVM and ANN. The network PDR also demonstrated an improvement of 45.33% and 51.81% using threat prevention measures using SVM and ANN.

REFERENCES

1. Harjeet Kaur, VarshaSahni, Dr.ManjuBala, “A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review”, International Journal of Computer Science and Information Technologies, (IJCSIT), Vol. 4 (3), pp. 498-500, 2013.
2. Rao, R. L., Satyanarayana, B., & Kondaiah, “Performance of CBIDS on AODV Routing Protocol against Black hole attacks in MANET”, IJSRCEIT, vol. 3, no. 3, pp. 1637-1644, 2018.
3. Panda, N., & Pattanayak B. K., “Energy aware detection and prevention of black hole attack in MANET”, International Journal of Engineering and Technology (UAE), vol. 7 no. 26, pp. 135-140, 2018.
4. Pooja, V. S., Rohit, T., Reddy, N. M., & Sudeshna S., “Mobile Ad-hoc Networks Security Aspects in Black Hole Attack”, in 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA) , pp. 26-30, 2018, IEEE.
5. Farooq, M. U., Wang, X., Sajjad, M., & Qaisar S., “Development of Protective Scheme against Collaborative Black Hole Attacks in Mobile Ad hoc Networks”, KSII Transactions on Internet and Information Systems (TIIS), vol. 12 no. 3, pp. 1330-1347.
6. Patel, M., Sharma, S., & Sharan, D. (2013, April). Detection and prevention of flooding attack using SVM. In 2013 International Conference on Communication Systems and Network Technologies (pp. 533-537). IEEE.
7. N. Arya, U. Singh and S. Singh,”Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm”,. In 2015 International Conference on Computer, Communication and Control (IC4) IEEE, pp. 1-5, 2015.
8. P. Gupta, P. Goel, P. Varshney, and N. Tyagi, “Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET”, In Smart Innovations in Communication and Computational Sciences, Springer, Singapore, pp. 271-279, 2019.
9. T. A. Kolade, "A Scheme for detecting and mitigating cooperative black hole attack in AODV-based MANET routing protocol." PhD dissertation, 2018.
10. A. Adnan, A. B. Kamalrulniza, M. I. Channa, and A.W. Khan. "A secure routing protocol with trust and energy awareness for wireless sensor network", Mobile Networks and Applications, Vol. 21, No. 2. pp 272-285, 2016.
11. Jain, A. K., Tokekar V. & Shrivastava S., “Security Enhancement in MANETs Using Fuzzy-Based Trust Computation Against Black Hole Attacks”, in Information and Communication Technology, pp. 39-47, Springer, Singapore, 2018.
12. Chhabra, A., Vashishth, V., & Sharma, D. K., “A fuzzy logic and game theory based adaptive approach for securing opportunistic networks against black hole attacks”, International Journal of Communication Systems, vol. 31, no. 4, pp. 3487-3510, 2018.
13. Abdel-Azim, M., Salah, H. E. D., & Eissa, “IDS Against Black-Hole Attack for MANET”, IJ Network Security, vol. 20 no. 3, pp. 585-592, 2018

AUTHORS PROFILE

Mr. Vishal Walia did his Bachelor as well as Masters in Electronics and Telecommunication Engineering from IET, Bhaddal (Punjab Technical University, Jalandhar). He is currently a research scholar at IKG Punjab Technical University, Jalandhar.

His area of research are wireless and Mobile Communication, Fuzzy Logic, Neural Network and Optimization. He has published more than 30 research papers in National and International Journal of repute. He is a life member of ISTE.

Dr. Rahul Malhotra did his Bachelor of Electronics and Telecommunication Engineering from Amravati University Amravati, in year 2001. He did Masters of Technology in Electronics and Communication Engineering from Giani Zail Singh College of Engineering and Technology, Bathinda and Doctorate of Philosophy in the faculty of Engineering and Technology from Punjab Technical University in collaboration with Thapar University Patiala.

His area of research includes Evolutionary Computing Techniques, Wireless Communication systems. He started his professional career from HCL Technologies Bangalore and later he shifted to technical education industry, with elite educational groups of Punjab,

He specializes in Wireless Adhoc Networks, Fuzzy Logic, Neural Network and Optimization. He has published more than 110 research papers in National and International Journal of repute. He has guided more than 85 research thesis at Master’s level and completed 04 Doctoral level of Research. He is a Fellow Member of Institution of Engineers, Calcutta, Institution of Electronics and Telecommunication Engineering, New Delhi and senior member of CSI and ISTE.

He served as faculty Head of Electronics and Communication engineering Guru Gobind Singh College of Engineering and Technology Talwandi Sabo, Adesh Institute of Engineering and Technology, Faridkot since 2001 to 2012 to teach Graduate and Postgraduate level of Engineering courses. In year 2011, he started groundwork to establish a new venture of Adesh Group at Chandigarh, Adesh Institute of Technology, Chandigarh Campus, Gharuan Tricity, and in year 2012, he joined as Founder Director-Principal of the campus.