FUZZY BASED MALICIOUS NODES DETECTION IN MOBILE AD-HOC NETWORKS

Er. Harmeet Singh,Research Scholar, Department of Computer Science & Engineering, SBBS University, Jalandhar,M.8054139336

Dr.Vijay Dhir,Professor, Department of Computer Science & Engineering, SBBS University, Jalandhar,M.8558939400

***Abstract*— In this paper, a Fuzzy based detection system that detects different MANETs attacks is proposed. The proposed system makes use of cluster based architecture to properly organize the nodes in the network. The proposed system use concept of anomaly detection and misuse detection that is based on fuzzy rule sets. The proposed system also makes use of Multilayer Perceptron Neural Network. The Back propagation Neural Network and Feed Forward Neural Network are used to add the results of detection and show the different types of attackers. Advanced Sybil Attack Detection Algorithm is used for the detection of Sybil attack, Wormhole Resistant Hybrid Technique is used for detection of wormhole attack while signal strength and distance is used for detection of hello flood attack. A set of nodes are used for the experimental analysis; 16.54% of the nodes are detected as misbehaving nodes. Hello flood attack is detected at a rate of 98.70%; wormhole attack has a detection rate of 97. 60%; and Sybil attack has a detection rate of 97. 20%.**

Keywords: Fuzzy, MANET, Multilayer Perceptron Neural Network, Back propagation Neural Network, Feed Forward Neural Network, Intrusion Detection, Sybil, Hello flood, wormhole.

1.INTRODUCTION

Mobile ad-hoc network (MANET) is an IP based infrastructureless network of wireless machine and mobile nodes connected with radio. In operation of MANET, the nodes do not have a centralized mechanism of administration. MANET is also known for its properties of routeable network in which each node perform job of a "router" so as to forward traffic to other nodes in the network. Figure 1 shows the structre of MANET. The security of MANET is one of the research issue and in the past a large number of intrusion detection techniques have been develop for different types of attacks. In this paper we focus on detection of Wormhole, Hello flooding, and Sybil attack in MANET.[1,3,7,8]

***Er.Harmeet Singh,**, Department of Computer Science & Engineering, SBBS University,Jalandhar ,Gurdaspur,India, M.8054139336.*
***Dr.Vijay Dhir**, Department of Computer Science & Engineering, SBBS University,Jalandhar,Hoshiarpur,India, M.8558939400.*

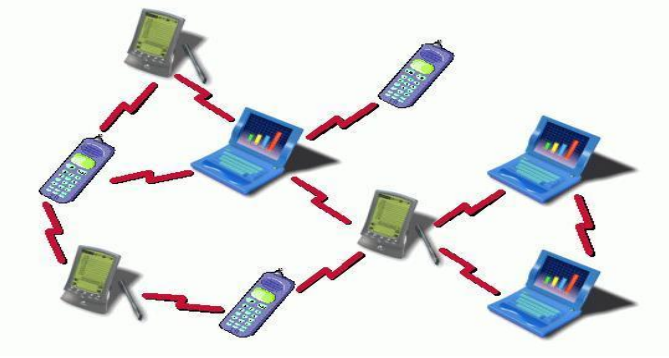

Figure 1: MANET

Numerous researchers have examined a module of hybrid module based on the merits of the both misuse detection and anomaly detection. The hybrid detection policy can recognize attacks with the highestcorrectness of the misuse detection and highest detection rate of anomaly detection. In this paper, we propose a fuzzy based Intrusion Detection System that utilizes a Multilayer Perceptron Neural Network (MPNN), which contains a feed forward neural network (FFNN) and back propagation neural networks (BPNN)to detect the Wormhole, Hello flooding,and Sybil attack with lower false alarm and greater detection ratio. [2,5,6,24]

2. FUZZY BASED HYBRID INTRUSION DETECTION SYSTEM

The proposed work of this paper aims for detecting Wormhole, Hello flooding, and Sybil attack in the Mobile ad-hoc network by using the hybrid Intrusion Detection System. The proposed work utilize fuzzy rules to identify the attackers of different types. Intrusion Detection System makes use of the benefits of both misuse detection and anomaly detection models for the detection of the Wormhole, Hello flooding, and Sybil attacks. The proposed Intrusion Detection System can obtain a greater detection rate and low positive rate. The proposed system can find and include new instances by the machine learning strategy of MPNN through practically when it undergoes about the unknown attacks. Intrusion Detection System proposed in

this research, contains FFNN and the BPNN as two important elements as shown in Figure 2. [2,16,19,18]

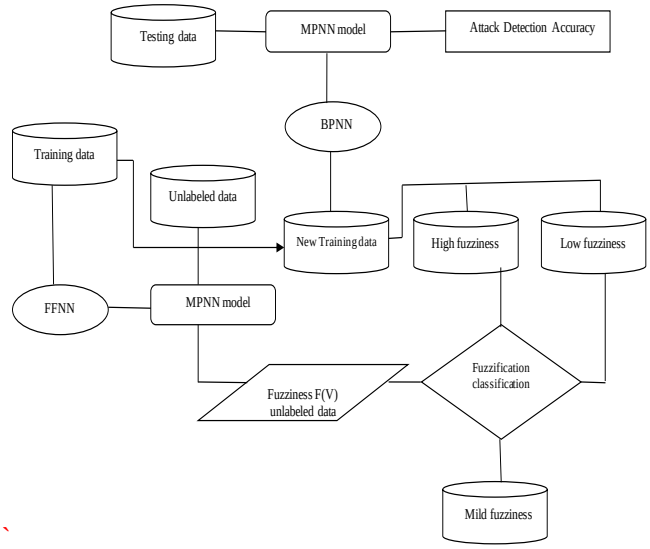

Figure 2: Proposed Intrusion Detection System

Intrusion Detection System first identify the data packets as abnormal or normal by making use of anomaly detection block. Different types of attacks are detected by misuse detection block covering the abnormal data packets. The output of the both detection blocks are combined making use of MPNN along with the fuzzy block. [11]
The anomaly detection model identify data packet as abnormal in the network once existing performance changes from that of normal. As a result, the anomaly detection normally recognizes the transmission along with abnormal data packets transmission which classify the erroneous nodes in the network. [23,18]

2.1 SYBIL ATTACK DETECTION

The Sybil attacker can get identities by either constructed identities (like creating arbitrary identifier) or by using identities that are stolen. The proposed detection mechanism detect new identity created by a Sybil attacker. The attacker joins the MANET with single identity and nodes do not vary their transmit power. Figure 3 shows a scenario of Sybil attack in MANET.
The Sybil attack is identified by making use of fuzzification method along with MPNN. The procedure is utilized for separating legitimate and Sybil node having the maximum mobility through the process of verification. The Intrusion Detection System stores RSSI value of every node in the table along with the time period. The system analyzesthis RSSI value to check whether first RSSI value stored is less than the threshold value or not. If it is not, Intrusion Detection Systeminclude node in attacker list along with updating its neighbor's list. [4]
The proposed Sybil detection method is combined with rule based anomaly detection module which utilizes fuzzy rules set so as to distinguish data units as either normalities or anomalies. If the fuzzy rules used by the proposed system are satisfied an anomaly is announced. The Sybil attack detection complies following processes: In this first process, neighboring nodes identify the data transmission path by utilizing the ranging-enabled scheme through hello packets. The data packets use RSSI signal; if they cross predefined range, then they have possibilities of getting affected by the malicious nodes due to weaker signal. So, the proposed work include the ranging estimation scheme in which each packet contain PHY header with certain bit called as the ranging bit.[9,10,12]

The next phase of proposed detection system make use of the concept of each node developing the table that compre locally calculated ranging estimation. First proposed detection system calculates the distance d_{ab}^{n} from the every other neighboring node.[22]

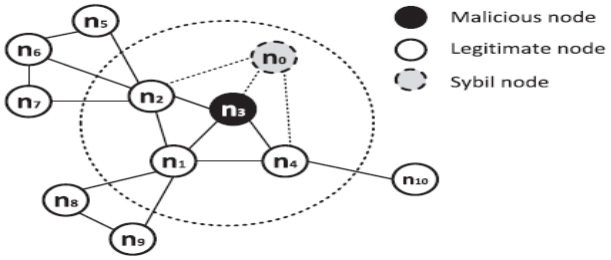

Figure 3: Sybil node detection analysis

Let d_{ab}^{n} represents detected distance between node n_a and node n_b as computed by the node n_a. The distance detection error is indicated as e error units. The d_{ab}^{e} represent the exact distance between the node n_a and the node n_b .Therefore, $(d_{ab}^{n} - \frac{n}{2}) < d_{ab}^{n} < (d_{ab}^{n} + \frac{n}{2})$ represent average for each node n_a, n_b.
In the next process each node in the MANET executes multiple distance matching verification. Node n_a equates the ranging measurements of each pair of nodes n_a and n_b ,signified in neighbor node list, i.e. for all $b, c \neq a$, $1 \leq b$

$$\text{If} \begin{cases} |\, d_{ab}^{n} - d_{ac}^{n} \,| < e\,, & \textit{then raise an alarm} \\ |\, d_{ab}^{n} - d_{ac}^{n} \,| \geq e\,, & \textit{else continue normal operation} \end{cases} \quad (1)$$

The above rules indicate that if node n_a determines that two nodes represented by n_b and n_c have a distance difference smaller than e quadratic metric units, then a Sybil attack is active. This node is identified and blacklisted. This could produce a false positive value in the fuzzy table.The third process of the proposed Sybil detection algorithm is a repeating process in which each node performs circular based Sybil attack detection which is further based on fuzzy rules along with a neural network.

2.2 DETECTION OF WORMHOLE ATTACK

For identifying wormhole attack, we use the Wormhole Resistant Hybrid Technique (WRHT) with Fuzzification method and MPNN. WRHT; a hybrid method based on Delphi and watchdog. The wormhole attack is shown in figure 4.

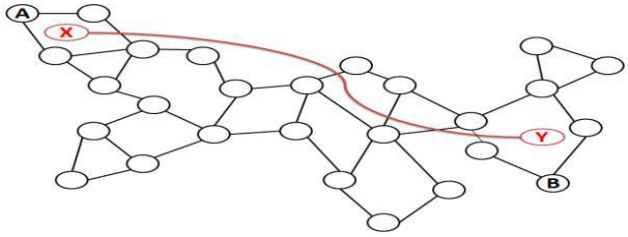

Figure 4: Wormhole tunnel

WRHT use drop of packetsinformationalong with each hop delay for wholenetwork route. WRHT allows source node to calculate the wormhole presence probability (WPP_p)of given path along with information of HC. Wormhole calculating is done by:

$$TDP_T = TDP_{REQ} + TDP_{REP} \quad (2)$$

where, TDP_{REQ} represent RREQ time delay probability. TDP_{REP} represent RREP time delay probability

$$(TDP_P) = 1 - (\prod_{j=1}^{n}(1 - TDP_j)) \quad (3)$$

where, TDP_jrepresent node j time delay probability.

$$(PLP_P) = 1 - (\prod_{j=1}^{n}(1 - PLP_j)) \quad (4)$$

where, PLP_jrepresent node j packet loss probability.
As two events are not mutually exclusive, the wormhole presence probability (WPPp) is defined as:

$$WPPp = \{TDPP + PLPP - (TDPP \text{ and } PLPP)\} \quad (5)$$

Calculated values of above equations are moved to FFNN. The fuzzy uses both anomaly and misuse detectors in order to estimate wormhole attack and malicious nodes are blacklisted.[13,14,20]

2.3 DETECTION OF HELLO FLOOD ATTACK

In hello flood attack malicious node disseminates hello packets with the help of a more powerful transceiver as compared to other nodes as shown in figure 5

Figure 5: HELLO flood attack

For minimizing the overhead of the communicationof the data packets, we consider the clustered based Mobile ad-hoc network. This is based on distance and RSS of the elected cluster head nodes. The following equation is used for estimating the distance:

$$Dist = sqrt[sq(x2-x1) + sq(y2-y1)] \quad (6)$$

In this equation (x1,y1) represent coordinates of the location of the destination node while (x2,y2) represent CH location coordinates attained through advertising HELLO packet.Receiving nodes in the network calculate $T_{RSS,}$ RSS threshold value, corresponding to each node radio range in MANET.Each node joins a CH if

$$(RSS < T_{RSS}) \;\&\&\; (Distance < T_{DIST}) \quad (7)$$

Node RSS and distance with threshold values are moved to the FFNN. The fuzzy based detector module make use of anomaly and misuse detectors for detecting Hello flood attack in the Intrusion Detection System.
Intrusion Detection Systemmake use of fuzzy based MPNN, which contsist of the FFNN and BPNN of supervised learning approach so as to identify the three attackers.[15,17,21]

3. DETECTION OF MALICIOUS NODES

This paper consider a clustered based Mobile ad-hoc network. The data data packets must demonstrate common patterns for the normal node behavior for the purpose of supervising the data packets. The paper make use of fuzzy rule based analysis in order to utilize development of the anomaly detection scheme, and such representing rules are determined by experts. The model of workflow is explained in the following three steps represented below:
Process 1: Evaluates the history of completetransmission of data packet. The data packets moving through the control nodeare forwarded to heads and further to the MPNN and subsequentlyto FFNN. Therefore, the previous data packets are classified into two types such as abnormal and normal.
Process 2: Intrusion Detection Systemin this phase select appropriate feature set, so as to look for recognition of key elements used to separate abnormal and normal packets.
Process3:this phase establishes rules for anomaly intrusion detection. Depending on resolution for the data packet, it selects best features so that fuzzy based rules are generated. Afterward, BPNN along with rule sets are deposited in the knowledge base.
The proposed research methodology try to find out the corresponding relationship between both input as well as output variables matching with corresponding weight. This is used to minimize the error rate occurring due to the interface for finding the highest accuracy. Therefore, proposed fuzzy based methodology along with MPNN, FFNN, and BPNN are used for obtaintaing maximum correctness level for the detection of attacks. In this paper, a MPNN is developed for the purpose of detection strategy mechanism of the proposed detection systemwith a hidden layer, input layer and an output layer. In this FFNN process, the determination of performance parameters and the error rate is done by application of the following formula

$$e_{r_i} = d_i - a_i \qquad (8)$$

In this equation, d_i and a_i denotes desired output and actual output respectively which is the result produced by MPNN. In the process of back propagation, MLP propagate the rate of error or signal in the network. As the proposed methodology in this paper, integrate anomaly and misuse detection schemes, we make use of abnormal packets as the input layer which are found by anomaly detection scheme.

Before the training data is forwarded to BPNN, this data is converted into analike form of BPNN. The data packets are converted into a binary stream value so as to BPNN which is kept at 0.1 to 1.0. The actual ratio of the learning is found from the simulation. Additionally, the values from the range of 0 to 1 are used as biases and weights. After training data are combined into BPNN, actual output results are obtained through mechanism of the FFNN.

The rectification and error value of output and hidden layers are assessed through the process of back propagation in MPNN. The anomaly detection scheme is used to identify the whole abnormal packets for the further verification, it is further forwarded to the scheme of misuse detection. It applies pre-processing step for the purpose of coverting abnormal packets to a binary. This binary value is forwarded to the scheme of misuse detection for the purpose of estimating the output value. The outcome is distributed to fuzzy module along with MPNN model so as to obtain best integration.

The proposed system make use of fuzzy module to make highest judgment so as to identify different types of attacsby mixing anomaly detection and misuse detection module.The fuzzy based system is usedfor supporting decision making model, by applying rules for aggregating outputs of two detection mechanisms. The FISperformance based on fuzzy membership (triangular)function along with fuzzy rules are applied to determine the suitable fuzziness on the input parameters. Further, this value is used for detecting the attackers types. The fuzzy values used as the input parameters as very high, high, very low, low, medium as represented in table 1. The hidden layer BPNN used are very long, long, veryshort, short, and mediumare also provided in table 1. The output parameters are produced as high fuzziness (Hello Flood attack), Low fuzziness (Sybil attack), and mild fuzziness (Worm hole attack).

We adopted MPNN to develop BPNN and FFNN mechanism of IDS, as this neutral network can manage a huge no. of data so as to continue the stability of the system and having capacity to attendthe different attackers. FFNN progress with detecting and estimating new types of attacks and that too simultaneously. The BPNN make use of cluster unknown MPNN learning mechanism that includes input layer, output layer and hidden layerrepresented in the Figure 6. As number of output nodes is established at the starting stage, numerous kinds of clusters may be produced by use of fuzzy based MPNN. This result in improved output nodes detection, in case when each of output nodecreates a extra type technique to detect attackers.

Each of the data packet that is unknown is introduced to the supervised learning mechanism of artificial intelligence so as to evaluationresultant points of each output. Afterward, it identifies output node results so as to evaluate corresponding output node winning value. If winning output node corresponding value is lesser than value of alertness then it indicates that inserted connected weight and data packet is not equal; therefore, the value does not match to corresponding cluster. In such case, next winning node results are checked to verify whether it can pass test of alertness. This would produce new output result node indicating identification of a new attack. Furthermore, simulation is used to definerequiredalertness value by use of sample data.

The fuzzy based proposed research methodology of rules in MPPN is defined in table 1. Let $T_r$be dataset of labeled examples, U be dataset of unlabeled examples, and $T_s$betesting dataset. First it utilize$T_r$to train data with the help of supervised FFNN classifier making use of N hidden nodes. The hidden node along with with BPNN classifier to get final output as sigmoid activation algorithm.The N membership with Vvector is achieved on eachsample of unlabeled data by investigating$U$ MPNN supervised learning method. The following membership vector with N unlabeled sample is applied to get Fuzziness $F(V)$

$$F(V) = -\frac{1}{n}\sum_{i=1}^{n}(\mu_i \log \mu_i + (1-\mu_i)\log(1-\mu_i)) \qquad (9)$$

Where, $V = \{\mu_1, \mu_2, \ldots, \mu_n\}$ is a fuzzy set.

Table1: Fuzzy rules based MPNN.

FFNN	BPNN	Fuzziness
Very- high	Very-long	Mid Fuzziness
Very- high	long	Mid Fuzziness
Very- high	Medium	Low Fuzziness
Very- high	Short	Low Fuzziness
Very- high	Very Short	Low Fuzziness
High	Very-long	Mid Fuzziness
High	long	Mid Fuzziness
High	Medium	Mid Fuzziness
High	Short	Low Fuzziness
High	Very Short	Low Fuzziness
Medium	Very-long	High Fuzziness
Medium	long	High Fuzziness
Medium	Medium	Mid Fuzziness
Medium	Short	Low Fuzziness
Medium	Very Short	Low Fuzziness
Low	Very-long	High Fuzziness
Low	long	High Fuzziness
Low	Medium	Mid Fuzziness
Low	Short	Mid Fuzziness
Low	Very Short	Mid Fuzziness
Very-low	Very-long	High Fuzziness
Very-low	long	High Fuzziness
Very-low	Medium	High Fuzziness
Very-low	Short	Medium
Very-low	Very Short	Medium

The fuzziness value is classified into low fuzziness, high fuzziness, and mid fuzziness. The samples that denote high

fuzziness and low fuzzinessare extracted. These values are included with the T_r so as to get T_{rnew} as revised datasetfor training of FFNN along with BPNN as represented figure 2 and 6.

The proposed approach, utilize KDD data sets so that pattern is coordinated. In order to determine clustered based Mobile ad-hoc network, the proposed approach utilize efficient training of MPNNfor minimizing utilization of energy by reducing dummy packets size. The pre-processing stage removes packets from the network so as to improve data strength utility. The size of these dummy variable packet is either below or above normal packets of data so as to reduce energy utilization. This will help in making adversary model to distinct between legitimate and fake packet

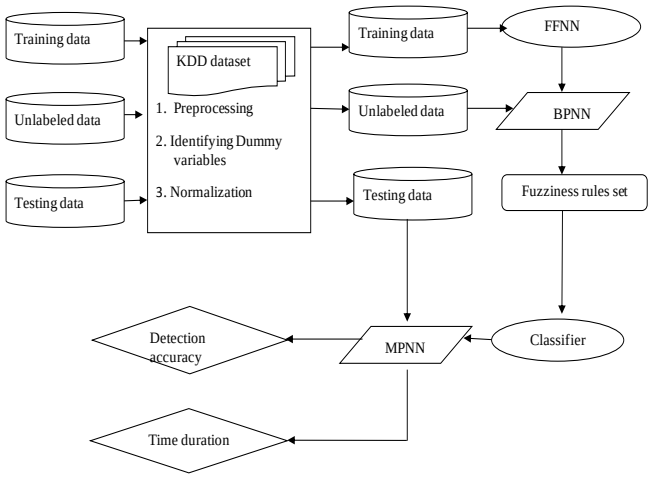

Figure 6: Fuzziness based MPPN

The performance of the proposed Intrusion Detection Systemcan be estimated by applying the following

Accuracy $$Acc = \frac{\sum_{i=1}^{C} TP_i}{N} \quad (10)$$

Recall $$Recall = \frac{TP_i}{TP_i + FN_i} \quad (11)$$

Average accuracy $$AAcc = \frac{1}{C}\sum_{i=1}^{C} Recall_i \quad (12)$$

Precision $$Preciosion_i = \frac{TP_i}{TP_i + FP_i} \quad (13)$$

F-measure $$FM_i = \frac{2 \cdot Recall_i \cdot Precision_i}{Recall_i + Precision_i} \quad (14)$$

Attacker accuracy $$Attacc = \frac{1}{C-1}\sum_{i=2}^{C} Recall_i \quad (15)$$

Attacker detection rate $$Adr = \frac{\sum_{i=2}^{C} TP_i}{\sum_{i=2}^{C} TP_i + FN_i} \quad (16)$$

where, *C* denotes number of classes,*N* stands for the number of examples and$TP_i$is the number of True Positive values of the i^{th} class, FP_i the number of False Positive values of the i^{th} class, $FN_i$is the number False Negative value of the i^{th} class.

4.SIMULATION-BASED IMPLEMENTATION AND EXPERIMENTAL RESULTS

We evaluate the performance of the proposed Intrusion Detection System in the Mobile ad-hoc network by using the NS2 network simulator version 2.33 (NS 2.33) with parameters specified in table 2. We estimate Hello flooding, Wormhole, and Sybil attack and their detection accuracy for the Mobile ad-hoc networks in the Intrusion Detection Systemwith Fuzzy Rules Based MPNN. In table 3, the results demonstrated that the misbehavior nodes are detected in the True Positive Rate (TPR) and False Positive Rate (FPR), which is detected with the MPNN using fuzzy logic mechansim.

Table 2: Simulation Parameters

Parameter	**Value**
Simulator	NS 2.3
Area	1600X900
Number of nodes	42
Routing protocol	DSDV
Packet size	512 bytes
Multilayer Perceptron	Two ray ground
Neural Network Model	Propagation model

The table 3 illustrates that detection rates under each level of node speed.Table 4 represents the detection rate and false negative for the attack of hello flood, wormhole and Sybil.

Table 3: Detection Rate

TPR	FPR
54% (Mid Fuzziness)	6% (Low Fuzziness)
58%(Mid Fuzziness)	13% (Low Fuzziness)
63% (High Fuzziness)	18% (Low Fuzziness)
79% (High Fuzziness)	19% (Low Fuzziness)

Table 4: Detection Ratio and False Negative Rate for three Attackers

Attack	Detection rate	False negative
Sybil Attack	97,20%	4,12%
Hello food attack	98,70%	2,22%
Wormhole attack	97,60%	5,16%

Figure 7, provides a scenario of the MANET having node 10 as selfish node. Node 10 is dropping packets and is detected as the attacker by the proposed system. Node 7 and node 41 as shown in figure 7 are detected as Sybil and wormhole attacks. Themalicious nodes are isolated from the network.

4.1 THROUGHPUT

Throughput is defined as total number of receiving packets at the destination and is calculated as :

Throughput = (Total no. of received packets at destination) / (time of simulation)

Throughput of the network is under attack, and proposed system is shown in Figure 8 in which proposed methodology results in the increase of throughput.

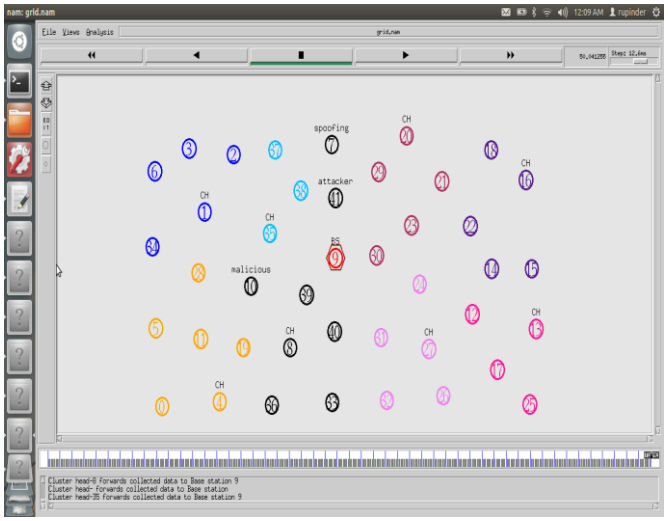

Figure 7: Detection of hello flood, Sybil, and wormhole attack.

4.2 PACKET DELIVERY RATIO (PDR)

PDR is ratio of the total received packets to the total packets generated and is calculated as:

PDR = (Packets received/packets generated) * 100

Proposed system PDR is shown in Figure 9 which shows increase of PDR.

4.3 PACKET LOSS

Packet loss is defined as the difference between the packets generated by the source node and the number of packets received by the destination node. Packet loss is calculated as:

Packet Loss = Generated Packets – Received Packets

Packet loss of proposed system is shown in Figure 10 which shows decrease in packet loss.

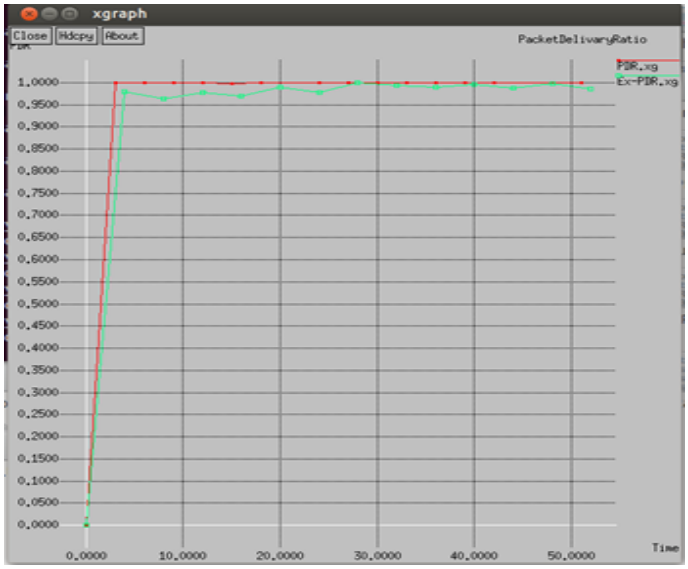

Figure 9: PDR of AIDS

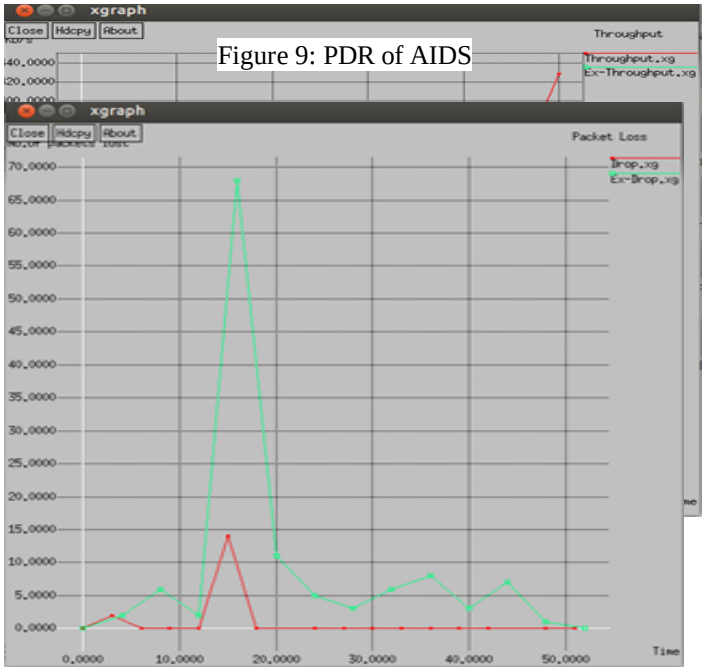

Figure 10: Packet loss of Intrusion Detection System

4.4 INTRUSION VS MEMBERSHIP

Figure 11 shows the relationship between the intrusion detection the membership function of proposed system.

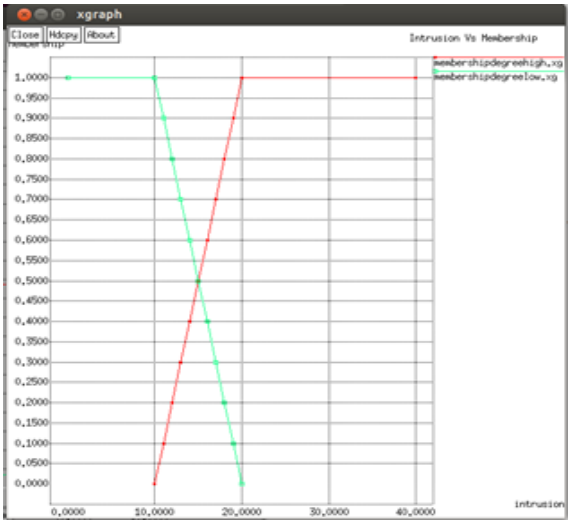

Figure 11: Intrusion Vs Membership of Intrusion Detection System

5. CONCLUSIONS AND FUTURE SCOPE

In this paper, we provide a jointprotection mechanism from wormhole, hello flood, and Sybil attack in mobile ad-hoc network. A fuzzy based hybrid intrusion detection model is proposed for MANET that makes use of both anomaly detection and misuse detection for the detection of attacks. The proposed system utilizes a Multilayer Perceptron Neural Networkcontaining feed forward neural network and back propagation neural networks of the supervised learning approach. The system make use of Fuzzy logic mechanism with anomaly and misuse detection technique to detect the Wormhole, Hello flooding, and Sybil attack. The grouping of these two techniques is used to providethe proposed Intrusion Detection System with a great detection rate and low false positive rate. The simulation results show that the propsed system is capable of performing low false positive rate and high true positive rate. The results provided in the paper also prove that the proposed system is extremely efficient for the parameters of packet loss, throughput, energy consumption, PDR, etc.

REFERENCES

[1] AkanshaSaini and Harish Kumar "Effect of Black hole attack on AODV Routing Protocol in MANET", International Journal of Computer Technology, Vol. 1, no 2, December 2010.

[2] EktaKamboj, "Detection of black hole on AODV in MANET using fuzzy" Journal of current computer science and technology, vol. 1, no. 6, pp 316-318, 2011.

[3] Ganapathy S, Yogesh P and Kannan A "Intelligent agent based Intrusion Detection System", Hindawi Publishing Corporation, Computational Intelligence and Neuroscience, 2012.

[4] Hu Y, Perrig A and Johnson B, "A Secure on Demand Routing Protocol for Ad Hoc networks", Proceeding of MobiCom, pp. 23-28, September 2002.

[5] Hu Y, Perrig Y and Johnson B, "Rushing attack and Defences in Wireless Ad Hoc Networks Routing Protocols", Proceeding of 2nd ACM workshop on Wireless Security, New York, 2003.

[6] Jungwon Kim and Peter J. Bentley "The Artificial Immune System for Network Intrusion Detection: An Investigation of Clonal Selection with a Negative Selection Operator", 2001.

[7] Kurosawa S and Jamalipour A, "Detecting Black hole Attack on AODV- based Mobile Ad Hoc Networks", International Journal of Network Security , Vol. 5, November 2007.

[8] Nadeem A and Howarth M, "Adaptive intrusion detection & prevention of Denial of Service", Proceeding of ACM 5th International Wireless Communication Conference, Germany, June 2009.

[9] Padilla E, Aschenbruck N, Martini P and Tolle J, "Detecting Black Hole Attack in Tactical MANETs using Topology Graph", Proceeding of 32nd IEEE Conference on Local Computer Networks, 2007.

[10] Pirrete M and Brooks M, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defence", International Journal of Distributed Sensor Networks, Vol.2, No.3, pp. 267-287, 2006.

[11] PoonamYadav, Rakesh Kumar Gill and Naveen Kumar, "A Fuzzy Based Approach To Detect Black Hole Attack", International Journal Of Soft Computing, ISSN: 2231-2307, vol. 2, no. 3, July 2012.

[12] Revathi B, Geetha D, "A Survey of Cooperative Black and Gray hole Attack in MANET", International Journal of Computer Science and Management Research, Vol 1, no 2, September 2012.

[13] ShanshanZheng, Tao Jian and John S: "Intrusion Detection of in-band wormholes in MANET using advanced statistical methods", IEEE 2008.

[14] SrinivasMukkamala, Guadalupe Janoski, Andrew Sung "Intrusion Detection Using Neural Networks and Support Vector Machines", in IEEE International Conference on Neural Networks, pp. 1702-1701, 2002.

[15] Steve Hofmeyr at all, "Intrusion Detection Using Sequences of Systems Call", Journal Of Computer Security, vol 6, pp 151-180, 1998.

[16] Susan Bridges and Rayford Vaughn, "Fuzzy Data Mining and Genetic Algorithms Applied To Intrusion Detection", Proceedings 23rd National Information Security Conference, pp 1-19, October 2000.

[17] Van Der Vorst H A, "Computational Methods for Large Eigenvalue Problems", in Handbook of Numerical Analysis, vol. 8, pp. 3-179, 2002.

[18] Vijayan R, Mareeswari V and Ramakrishna K "Energy based trust solution for detecting selfish nodes in MANET using fuzzy logic", International Journal of Research in computer, vol. 2 No. 3, June 2011.

[19] Wang Yu, "Using Fuzzy Expert System based on Genetic Algorithm for Intrusion Detection System", April 2009.

[20] Xiaopeng G and Wei C, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad Hoc Networks," Proceeding of IFIP International Conference on Network & Parallel Computing, 2007.

[21] Yi P, Dai Z and Zhang S, "Resisting Flooding Attack in Ad Hoc Networks", Proceeding of IEEE Conference on Information Technology: Coding and Computing", Vol.2, pp. 657-662, 2005.

[22] J Singh, O Singh and R Singh,"MRWDP: Multipoint Relays Based Watch Dog Monitoring And Prevention For Blackhole Attack In Mobile Adhoc Networks" Journal of Theoretical and Applied Information Technology, Vol. 95,pp.19,2017.

[23] J Singh, O Singh and R Singh," An Intelligent Intrusion Detection and Prevention System for Safeguard Mobile Adhoc Networks against Malicious Nodes" Indian journal of Science & Technology,Vol.10,pp.05,2017.

[24] Vijay .Dhir, R.Kumar and V.Joshi "Performance comparison of routing protocols in mobile ad hoc networks" International Journal of Engineering Science and Technology,Vol.2, pp. 3494-3502, 2010.

Er. Harmeet Singh, Assistant Professor at Sant Baba Bhag Singh University,Khila Jalandhar,Harmeet Singh Completed B.tech in computer science & Engineering at S. Sukhjinder Singh College of Engg. & Technology and M.tech in computer Science & Engineering at K.C. College of Engineering and Information Technology, Nawanshahr ,Ph.D* (Computer Science & Engg.) at Sant Baba Bhag Singh University Khila Jalandhar.

Dr. Vijay Dhir Professor and Director R & D at Sant Baba Bhag Singh University,Khila Jalandhar, Ph.D (Computer Science & Engineering)