A New Intrusion Detection System Based on Soft Computing Techniques Using Neuro-Fuzzy Classifier for Packet Dropping Attack in MANETs

Alka Chaudhary[1], V. N. Tiwari[2], and Anil Kumar[1]

(Corresponding author: Alka Chaudhary)

Department of Computer Science and Engineering, Manipal University[1]
Department of Electronics and Communication Engineering, Manipal University[2]
Jaipur 303007, India
(Email: alkachaudhary0207@gmail.com)

(Received Mar. 6, 2014; revised and accepted Sept. 16 & Dec. 22, 2014)

Abstract

Due to the advancement in communication technologies, mobile ad hoc networks are very attractive in terms of communication because mobile nodes can communicate without the relay on predefined infrastructure. Therefore, some complex properties of mobile ad hoc networks make it more vulnerable to internal and external attacks. From the security perspective, prevention based methods such as encryption and authentication are not considerably good solution for mobile ad hoc networks to eliminate the attacks so that intrusion detection systems are applied as a keystone in these types of networks. The main objective of intrusion detection system is to categories the normal and suspicious activities in the network. This paper proposed a novel intrusion detection system based on soft computing techniques for mobile ad hoc networks. The proposed system is based on neuro-fuzzy classifier in binary form to detect, one of vey possible attack, i.e. packet dropping attack in mobile ad hoc networks. Qualnet Simulator 6.1 and MatLab toolbox are used to visualize the proposed scenarios and evaluate the performance of proposed approach in mobile ad hoc networks. Simulation results show that the proposed soft computing based approach efficiently detect the packet dropping attack with high true positive rate and low false positive rate.

Keywords: Fuzzy inference system (FIS), IDS, MANET, neuro-fuzzy, packet dropping attack soft computing

1 Introduction

Mobile ad hoc networks (MANETs) are very prominent research area for researchers because MANETs have more vulnerabilities than the conventional networks. MANETs nodes can able to form the network without rely on predefined infrastructure or fixed infrastructure. Due to this nature of MANET, it is widely employed in many applications, E.g. military areas, disaster relief management virtual conferences, neighborhood area networks and likewise many others promising fields. MANETs are very prone to intrusions or attacks than the wired networks because of lack of clear line of defense, wireless links, no centralized points and dynamic topologies [9]. This paper focused on a very particular attack, i.e. packet dropping attack based on ad hoc on-demand distance vector (AODV) routing protocol [4]. In terms of security, prevention based techniques are not enough for MANETs security so that intrusion detection system (IDS) is used as a second line of defense for these networks.

When any set of actions make an effort to compromise with the security properties such as confidentiality, integrity, availability of resources and repudiation then these actions are called intrusions and detection of such intrusions are known as intrusion detection system. The primary objective of IDS is to categories the normal and suspicious activities in the network [26].

The basic functionality of IDS depends on three main components such as data collection, detection and response. The data collection component is responsible for collecting the data from various sources such as system audit data, network traffic data, etc. Detection module is responsible for analyzing the collected data to detect the intrusions, and if any suspicious activity detected than initiates the response by the response module.

There are three detection methods presented in the literature such as misuse based, anomaly based and specification based techniques [2, 3, 18]. The first method, misuse based detection systems detect the intrusions on the behalf of predefined attack signature. Second, anomaly-based detection technique detects the intrusion on bases of normal behavior of the system. Defining the normal behavior of the system is a very challenging task because behavior of system can be changed time to time. This technique can detect the unknown or new attacks but with high false positive rates. The third technique is specification - based intrusion detection. This technique specified or defined the set of constraints on a specific protocol and then detects the intrusions at the run time violation of these specifications. Therefore, defining the specification is very time consuming job in this technique.

Normally there are three basic types of IDS architecture in literature: Stand-alone or local intrusion detection systems, Distributed and Cooperative intrusion detection systems, Hierarchical Intrusion Detection Systems [18]. This paper emphasized the local intrusion detection system (L-IDS) and distributed and cooperative intrusion detection system (DC-IDS) based on neuro-fuzzy classifier for detection of packet dropping attack in MANETs that are discussed in Section 5.

There are many IDSs have been developed for wired networks but these IDSs could not be employed on MANETs because of its complex characteristics. Accordingly, researchers have been designed new IDSs for MANETs domain [18]. However, this paper enforces the use of soft computing methods in MANETs.

Soft computing is viewed as an emerging method for computing which present the notable potentiality of human mind to understand and learn in the situation of imprecision and uncertainty [25]. Generally, soft computing admits three main components such as neural networks, fuzzy logic and genetic algorithms.

Many of the soft computing techniques have proved their applicability in the field of intrusion detection in wired networks. Recently, many of the researchers are emphasizing on soft computing techniques for intrusion detection in MANETs so that some of the IDSs based on soft computing techniques have been developed for MANETs [5, 11, 12, 13, 17, 20, 21, 22, 23].

Consequently, mostly fuzzy systems construct their fuzzy rules on the bases of human expert knowledge so that these systems have lake adaptation. Moreover, several methods have been proposed for automatically formation of fuzzy rules in fuzzy systems, i.e. fuzzy-genetic and neuro-fuzzy [1, 14]. This paper develops a new intrusion detection system based on neuro-fuzzy classifier. The main contribution of this work is to build the classifier in binary form for separating the normal and abnormal activities in MANETs. For this aim, ANFIS is employed as a neuro-fuzzy classifier in the binary form and subtractive clustering is utilized for defining the initial fuzzy rules and membership functions.

The rest of the sections of this paper are organized as follows: Section 2 defines AODV (Ad Hoc on Demand Distance Vector) routing protocol and presented the target attack related to this research. Section 3 elaborates the fuzzy inference systems, neuro-fuzzy concepts and particularly, ANFIS (Adaptive Neuro-Fuzzy Inference System). This section also describes the subtractive clustering technique. Section 4 presents the data extraction on specific features by Qualnet simulator 6.1 in MANET environment for the implementation of proposed method. In Sections 5 and 6, explain the proposed system and evaluate the performance of proposed system in local and cooperative environment. Finally, conclude the paper in Section 7.

2 Aodv and Packet Dropping Attack

One of the widely used routing protocol in MANETs is ad hoc on demand distance vector (AODV) [15]. We have used AODV routing protocol in this research. One of very particular attack on MANETs is packet dropping attack that is considered in this research. The full description of attacks on MANETs is elaborated in [19]. Packet Dropping Attack: In a packet dropping attack, an attacker or malicious node(s) drop the data packets not destined for disturbing the services or operations of the network [19]. For achieving their objective, malicious or attacker node(s) required to be on a routing path or take a part of routing operations so that attacker nodes have a very small reason to drop the RREQ, RREP and RERR packets. We assumed in this research that the attacker nodes do not drop the RREQ, RREP and RERR packets of AODV routing protocol. Due to dropping data packets, network performance can reduced in terms to retransmit the data packets or new efficient route discovery. This attack can prevent the communication between nodes in the network.

In this research during simulation, attacker nodes continuously drop the data packets in every 1 sec intervals. Generally in wired networks, the packet losses happen due to congestion. In MANETs, due to its complex characteristics there are some other reasons such as congestion, mobility and wireless links transmission error to drop the packets. As in MANETs, mobility is the major cause to lose the data packets on AODV [10]. That's why this research concentrates to differentiate the packet dropping due to the mobility from the packet dropping due to malicious nodes in MANETs.

3 Fuzzy and Neuro-fuzzy

Fuzzy logic is one of very important component of soft computing that can able to deal with uncertainty and impreciseness drived from human logical thinking or reasoning. Fuzzy logic is able to handle the multi valued logic of fuzzy set theory between the ranges of 0 to 1 and it gives the decisions in degrees form rather than yes or no terms [23]. IF-then- else based fuzzy rules can specify the every situation in the network for detecting the intrusions or attacks. Fuzzy inference system (FIS) is based on fuzzy rules for taking the decisions towards fuzzy reason-

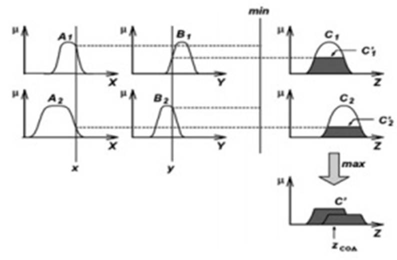

Figure 1: The Mamdani fuzzy interference system (MFIS) with min and max operators [8]

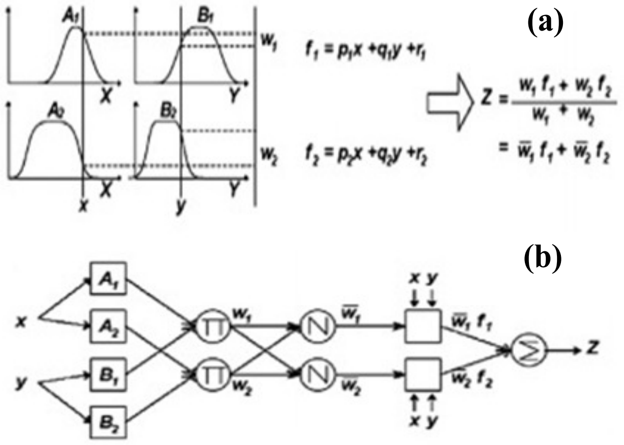

Figure 2: (a) Presents the Sugeno model fuzzy reasoning [8]. (b) Equivalent ANFIS structure [8]

ing. Some familiar fuzzy inference systems are proposed in the literature [8].

Mamdani FIS is shown in Figure 1. This is used defuzzification module that converts the fuzzy values to crisp values in terms of output. But, it is time consuming procedure. Takagi et al. suggested an approach to render the fuzzy rules from dataset [8] and is depicted in Figure 2(a). It is more efficient towards computation and also more suitable with adaptive techniques. Here, defuzzification is done by using weighted average.

There are several hybrids of soft computing approaches, where hybrid of neural and fuzzy has very popularity in many domains so that a very popular method has been proposed by Jang et al., which is known as ANFIS (Adaptive neuro-fuzzy inference system) [8].

In any modelling situation where nobody can't discover and recognize the membership functions and parameters linked with member functions for the large or vast data set. In this situation ANFIS is useful. It suggests a procedure for fuzzy modelling in respect of learning the information from a given dataset for computing the parameters of membership functions that permit the associated FIS to track or handle in best way of given input and output data. The membership functions related parameters will alter according to the procedure of learning. ANFIS can employ back propagation algorithm or aggregation of back propagation algorithm and least square estimation for the estimation of parameters related with membership functions. Figure 2(b) describes the ANFIS architecture [8]. This paper utilized the subtractive clustering method for determining the initial number of fuzzy rules and membership functions. However, ANFIS is applied for further fine tuning of these functions. Subtractive clustering [6] is quick, single pass algorithm for computing the clusters and cluster centres from a given dataset. Subtractive clustering is an extension of mountain clustering method that is indicated by Yager in [24].

According to the cluster information which is received by this algorithm is utilized to discover the initial rules and membership functions that are responsible to form the FIS. In this research work, FIS structure is received through subtractive clustering to cover the all features space. So this paper selected the subtractive clustering technique for evolving the numbers of initial fuzzy rules.

4 Features Selection and Dataset

"Features" are the spectacular attributes that are employed as inputs to our suggested system. For evolving of the better results, the selection of appropriate features is most important. Our proposed system has concentrated on features related to the packet dropping attack. Our proposed features are illustrated in Table 1, those are asserted on each node in the network through the AODV routing protocol. Basically this paper is emphasized to detect packet dropping attack through malicious nodes so that it permit to focuses a rich set of features for demonstrated the efficiency of proposed IDS.

The features are collected based on two categories, i.e. mobility related features and packet related features. Mobility related features devote the information regarding the reflection of mobility model for each node or network. Moreover, some features such as added neighbors; remove neighbors directly reflect the mobility of a node. Packet related features admit the information about the frequency of the routing protocol control packets for sent (RREQ), received (RREP) and forwarded at each time interval. However, some features are definitely presented the signature of particular attack e.g. detection of the packet dropping attack is possible through the "Dropped_datapkts" feature [17]. There is no requirement of communication amongst the mobile nodes during the collection of data, since totally selected features are local to each node [17]. This paper used the Qualnet simulator 6.1 [16] for extracting the data based on selected features to analyse the results of proposed system. Table 2 presented the list of parameters that have been set during the simulation by using Qualnet simulator and Table 3 is given the details of datasets in training, checking phases with simulation time 1,000s and testing with 800s

Table 1: The list of selected features

Abbreviations of Features	Explanations
Enum_dataPks_Initd	No. of data packets sent as source of the data by this node
num_dataPks_ fwrd	No. of data packets forwarded by this node
num_dataPks_ recvd	No. of data packets sent as destination of the data by this node
Num_ rep_ recvd_asSrce	No. of RREP packets received as source by this node
num_rep_initd_asDest	No. of RREP packets initiated from the destination by this node
num_rep_initd_asIntermde	No. of RREP packets initiated from the an intermediate node
num_rep_fwrd	No. of RREP packets forwarded by intermediate nodes
Num_ rep_ recvd	No. of RREP packets received by this node
num_req_recvd_asDest	No. of RREQ packets received as a destination for this node
num_err_ fwrd	No. of RERR packets forwarded by this node
num_err_ initd	No. of RERR packets initiated as this node detect the link break
num_routes	No. of routes added to the route cache
num_err_ recvd	No. of RERR packets received by this node
num_req_ initd	No. of RREQ packets initiates by this node
num_req_receivd	No. of RREQ packets received to this node
Num_brknLinks	Total no. of broken links
Dropped_datapkts	Calculates not forwarded data packets through this next node
num_addNbrs	No. of added neighbors of node during simulation time
num_rmveNbrs	No. of remove neighbors of node during simulation time
num_nbrs	No. of neighbors of node during simulation time

for neuro-fuzzy classifier based IDS in MANETs.

Table 2: Data samples in training, checking phase with simulation time 1,000s and for testing with 800s

Distributions of Data Samples	Class Normal	Class Attack
Training	12,000	12,000
Checking	3,000	3000
Testing	2,500	2500
Total	17,500	17500

Table 3: Simulation parameters list

Simulation Parameters	
Simulation time	1000s (Training) and 800s (Testing)
Mac Type	IEEE 802.11
Radio type	802.11b
Routing protocol	AODV
Antenna	Omni directional
No. Of Channels	One
Channel frequency	2.4 GHz
Packet size	512 bytes
Simulator	Qualnet 6.1
Energy Model	Generic
Path loss model	Two Ray
Pause time	30 second
Battery model	Linear model
Mobility speeds	0 to 25 mps
Batter Charge Monitoring	Interval 60 Sec.
Traffic type	CBR
Simulation area	1500m $\times 1500m$
Number of nodes	15 and 30 nodes
Mobility	Random Way Point
Malicious Nodes	4

5 Our Proposed Approach

The main motivation towards this proposed work to provide a framework for using hybrids of soft computing techniques, i.e. neuro-fuzzy to build the binary classifier that can act batter than the single soft computing technique.

In this section, we describe the proposed architectures of binary neuro-fuzzy classifier based intrusion detection system for MANETs which is depicted in Figure 3 and also includes data collection, detection and response modules. We utilized the feature list referred in Table 1, as the inputs for proposed IDS. Input patterns are labelled with 0 and 1 where 0 for normal and 1 for attack input data patterns for the point of view binary classifier

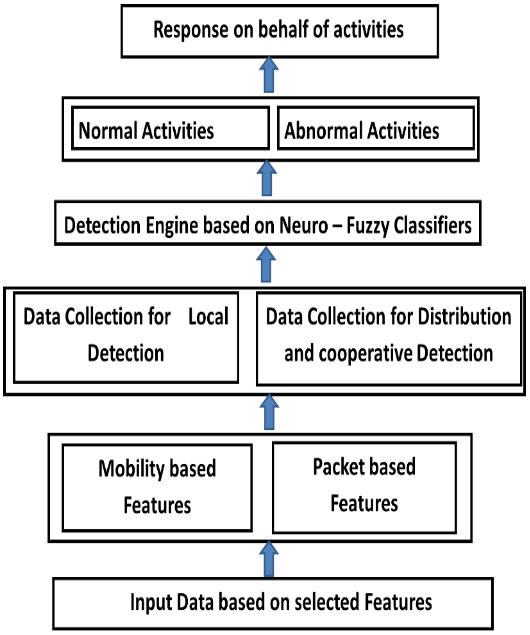
Response on behalf of activities
Normal Activities
Abnormal Activities
Detection Engine based on Neuro – Fuzzy Classifiers
Data Collection for Local Detection
Data Collection for Distribution and cooperative Detection
Mobility based Features
Packet based Features
Input Data based on selected Features

Figure 3: Architecture of proposed intrusion detection system

in MANETs. This paper described the two architectures of proposed binary neuro-fuzzy classifier based intrusion detection system, i.e. local, and distributed and cooperative.

In local intrusion detection system (L-IDS), each mobile node has an IDS agent in the network and detects the attacks on the bases of their own decision without the collaboration with other nodes. Moreover, in distributed and cooperative intrusion detection system (DC-IDS), each mobile node in the network has an IDS agent and detects the attacks on the bases of communication with other nodes to exchange the information, to share the decisions and finally to agree on responses with other nodes [18]. In this paper for DC-IDS, nodes communicate with their one hop away neighbors nodes to reach the decision that there is any malicious activity is available in MANETs or not.

For developing the L-IDS based on neuro-fuzzy classifier, 24,000 data patterns are used in training phase and 6,000 corrected label data patterns are used for checking phase to validate the model. As in Table 3 presented that 5,000 patterns are used for testing data that are not corrected label to test the model.

This paper used the subtractive clustering approach with neighborhood radius $r_a = 0.5$ to partition the training dataset and build the automatic initial fuzzy rules to make the fuzzy inference system (FIS) structure for training of ANFIS.

Hence, seven fuzzy rules and seven membership functions (Gaussian type) were received for each input. For further fine tuning and adaptation of membership functions, training dataset was applied for training of ANFIS and checking dataset was employed to check the validation of model since after some time in training phase, the model begins the over fitting with training dataset so that generated FIS acts bias with other independent datasets.

The employed ANFIS holds 272 nodes and total no. of fitting parameters are 364, in which premise parameters are 238 and consequent parameters are 126. The root mean square error (RMSE) of training and checking dataset are 0.34157 and 0.38461 after learning of 50 epochs.

As we discussed that the architecture of ANFIS gives simply one output so that here in this work the output of ANFIS architecture is mention by the class number, where class number 0 refers the normal activities and 1 presents the attacks.

For evolving the distributed and cooperative based intrusion detection system, the features for neighbor node is also available in Table 1 so that each mobile node can exchange the information about intrusions to their one hop away neighbor nodes through secure communication channels. The performance of training and testing of this architecture after 50 epochs is given in the Table 4. The performance of L-IDS and DC-IDS is demonstrated in Table 4.

The ANFIS output is not essential to provide the exact class number, i.e. 0 or 1 so that it may require the approximate value of class number. Due to this reason, a parameter is used to rounding off the given (output) number and provide the integer value (either 0 or either 1) to us. As per earlier mentioned in Section 4, ANFIS used the further fine tuning and adaptation of membership functions. Figure 4 shows the initial and final membership functions of some input features during ANFIS training phase.

There were developed some standard metrics, i.e. true positive rate and false positive rate for evaluating the performance of intrusion detection system [18]. Table 5 depicted the true positive rate and false positive rate after 50 epochs of training and checking dataset at $\mu = 0.5$.

6 Results

From the results point of view in this paper, two different ways of testing have been applied. This paper used all patterns of packet dropping attack without corrected labelled dataset to test our proposed neuro- fuzzy classifier based local intrusion detection system and cooperative detection system. Table 4 shows the detection rates, i.e. true positive rate and false positive rate of L-IDS and DC-IDS under 15 and 30 nodes with varied traffic rate and mobility speeds. Figures 5, 6 presented the true positive rate of L-IDS and DC- IDS and Figures 7, 8 presented the false positive rate in respect of L-IDS and DC- IDS. From the results it noticed that neuro-fuzzy classifier based DC-IDS increases the true positive rate and decreases the false positive rate in terms of L-IDS. But in DC-IDS, exchang-

Table 4: Shows the detection rates of L-IDS and DC-IDS

No of Nodes	Traffic	Mobility	Local Detection(%)		Distributed and Cooperative Detection(%)	
			TPR	FPR	TPR	FPR
15	high	low	98.0	1.31	98.52	1.12
15	low	low	99.84	0.47	99.85	0.31
15	low	high	99.90	0.82	99.95	0.79
15	medium	medium	99.53	1.50	99.73	1.37
30	high	low	98.48	1.76	98.53	1.53
30	low	low	99.87	0.89	99.85	0.83
30	low	high	0.99	99.97	5.5	0.95
30	medium	medium	99.61	99.75	5.5	2.00

ing the information between the neighbors nodes may be consumed more energy and bandwidth over L-IDS so an alternative solution for DC-IDS is that if any node having the symptoms about the suspicious activity present in the network, at that moment this node exchange the information their neighbor nodes.

In this paper, the receiver operating characteristics (ROC) analysis is used in regards of the parameter for presenting the effect on the true positive rate and false positive rate. Basically this ROC analysis is made for evaluating the performance of neuro-fuzzy classifier in respect of parameter. For discovering the variation between true positive rate and false positive rate, we varied the value of parameter between the 0 to 0.5 and plotted the coordinate points in respect of (FPR, TPR) μ [7].

7 Conclusion

In this paper, we have proposed a novel intrusion detection system based on neuro-fuzzy classifier in binary form for packet dropping attack in mobile ad hoc networks. In terms of IDS architecture, we have described two types of architectures based on neuro fuzzy classifier, i.e. local, and distributed and cooperative. From the results it's noticed that L-IDS and DC-IDS both the systems presented good performance to detect the packet dropping attack. The proposed architectures of IDS give the output in form of 0 or 1 where 0 shows the normal pattern and 1 presents the abnormal pattern so that in this paper, output 1 means malicious nodes are presented in the network. In future, we are concentrating to detect all type of attacks in MANETs environment.

Acknowledgments

This work is partially supported by government of India vide Dst/tsg/nts/2012/106, we acknowledge A.N.TOOSI (Department of Computing and Information System), University of Melbourne for their useful suggestions.

Table 5: True positive rate (TPR) and false positive rate (FPR) of training and checking dataset at $\mu = 0.5$

Data Set	**TPR%**	**FPR%**
Training	99.82	0.61
Checking	98.1	1.7

References

[1] M. S. Abadeh, J. Habibi, and C. Lucas, "Intrusion detection using a fuzzy genetics-based learning algorithm," *Journal of Network and Computer Applications*, vol. 30, pp. 414–428, 2005.

[2] A. Chaudhary, A. Kumar, and V. N. Tiwari, "A reliable solution against packet dropping attack due to malicious nodes using fuzzy logic in MANETs," in *International Conference on Optimization, Reliabilty, and Information Technology (ICROIT'14)*, pp. 178–181, 2014.

[3] A. Chaudhary, V. N. Tiwari, and A. Kumar, "Analysis of fuzzy logic based intrusion detection systems in mobile ad hoc networks," *BVICAM's International Journal of Information Technology*, vol. 6, no. 1, pp. 690–696, 2014.

[4] A. Chaudhary, V. N. Tiwari, and A. Kumar, "Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc network," in *IEEE International Advance Computing Conference (IACC'14)*, pp. 256–261, 2014.

[5] A. Chaudhary, V. N. Tiwari, and A. Kumar, "A cooperative intrusion detection system for sleep deprivation attack using neuro-fuzzy classifier in mobile ad hoc networks," *Computational Intelligence in Data*, vol. 2, pp. 345–353, 2015.

[6] S. L. Chiu, "Fuzzy model identification based on cluster estimation," *Journal of Intelligent and Fuzzy Systems*, vol. 2, no. 3, pp. 267–278, 1994.

[7] J. Gomez and D. Dasgupta, "Evolving fuzzy classifiers for intrusion detection," in *Proceedings of the*

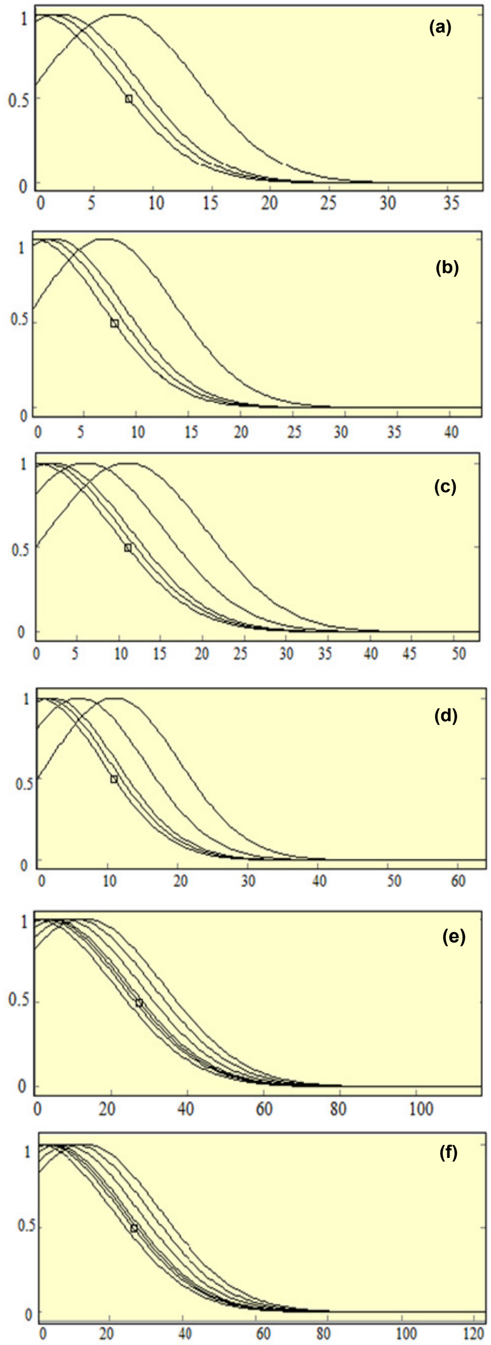

Figure 4: Initial and final membership functions of some input features during ANFIS training phase. (a) Before training, MFs of input feature 6 in L-IDS. (b)After training, MFs of input feature 6 in L-IDS. (c)Before training, MFs of input feature 11in L-IDS. (d) After training, MFs of input feature 11in L-IDS. (e) Before training, MFs of input feature 13in DC-IDS.(f)After training, MFs of input feature 13 in DC-IDS.(a), (c), (e) presents the initial membership functions before training phase and (b), (d), (f) final membership functions after training phase.

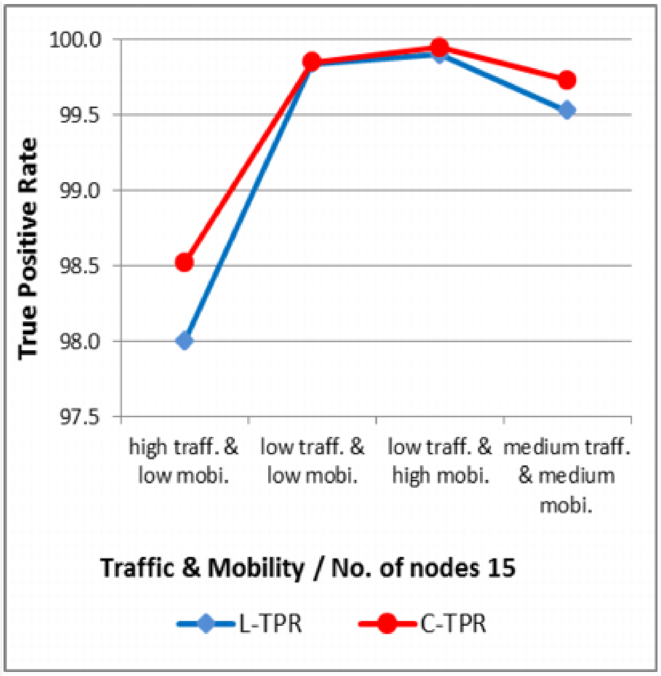

Figure 5: represents true positive rate under 15 nodes of L-IDS and DC-IDS

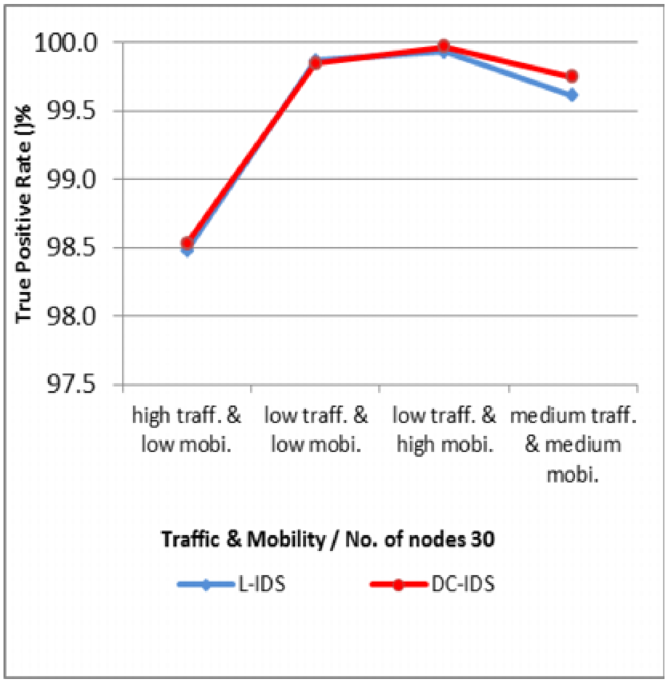

Figure 6: represents true positive rate under 30 nodes of L-IDS and DC-IDS

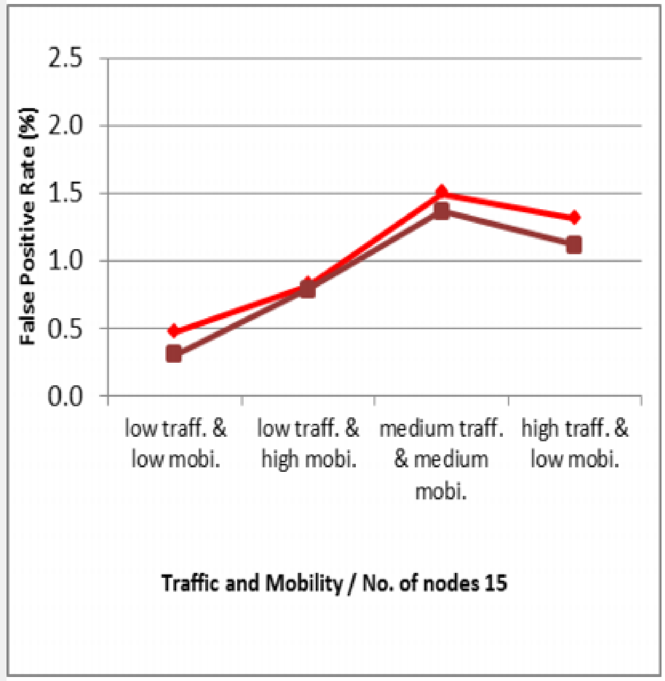

Figure 7: represents false positive rate under 15 nodes of L-IDS and DC-IDS

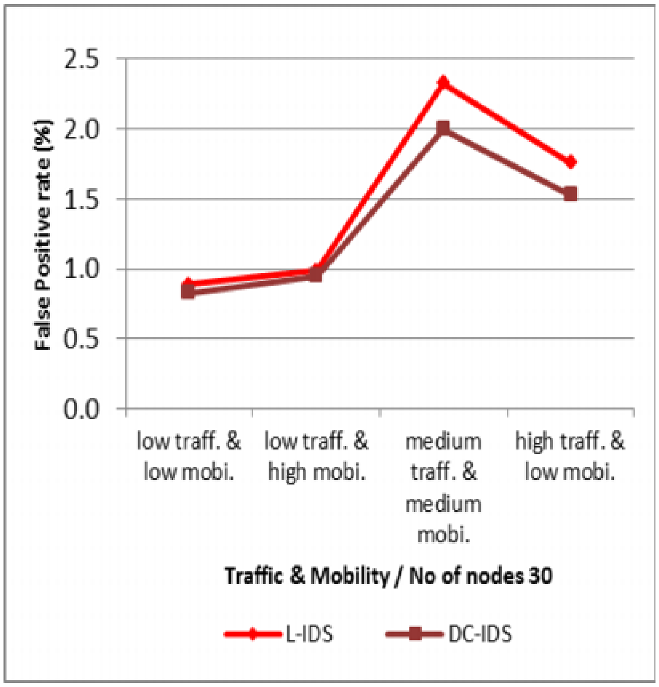

Figure 8: represents false positive rate under 30 nodes of L-IDS and DC-IDS

2002 IEEE Workshop on Information Assurance, vol. 6, pp. 1–8, 2002.

[8] J. S. R. Jang, C. T. Sun, and E. Mizutani, *Neuro-Fuzzy and Soft Computing - A Computational Approach to Learning and Machine Intelligence*, Prentice-Hall, 1996.

[9] Y. Li and J. Wei, "Guidelines on selecting intrusion detection methods in manet," in *Proceedings of the Information Systems Education Conference*, pp. 1–17, 2004.

[10] Y. Lu, Y. Zhong, and B. Bhargava, *Packet Loss in Mobile Ada Hoc Networks*, Computer Science Technical Reports, Report Number: 03-009, Purdue University, 2003.

[11] A. Mitrokosta, N. Komninos, and C. Douligeris, "Intrusion detection with neural networks and watermarking techniques for MANETs," in *IEEE International Conference on Pervasive Services*, pp. 118–127, 2007.

[12] Z. Moradi and M. Teshnehlab, "Intrusion detection model in manets using ANNs and ANFIS," in *International Conference on Telecommunication Technology and Applications*, vol. 5, 2011.

[13] Z. moradi, M. Teshnehlab, and A. M. Rahmani, "Implementation of neural networks for intrusion detection in MANET," in *International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT'11)*, pp. 1102–1106, 2011.

[14] D. Nauck and R. Kruse, "Nefclassmdash: a neuro-fuzzy approach for the classification of data," in *Proceeding of ACM Symposium on Applied Computing*, pp. 461–465, 1995.

[15] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the Second IEEE workshop on Mobile Computer Systems and Applications*, pp. 90–100, 1999.

[16] SCALABLE Network Technologies, "Qualnet simulator," Sept. 1, 2015. (`http://www.scalable-networks.com`)

[17] S. Sen and J. A. Clark, "A grammatical evolution approach to intrusion detection on mobile ad hoc networks," in *ProceedingsIn of the Second ACM Conference on Wireless Network Security (WiSec'09)*, pp. 95–102, 2009.

[18] S. Sen and J. A. Clark, *Guide to Wireless Ad Hoc Networks: Chap. 17. Intrusion Detection in Mobile Ad Hoc Networks*, pp. 427–454, Springer, 2009.

[19] S. Sen, J. A. Clark, and J. E. Tapiador, "Ad-hoc on-demand distance vector routing," in *Security Threats in Mobile Ad Hoc Networks, Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, pp. 127–147, 2010.

[20] M. H. Shao, J. B. Lin, and Y. P. Lee, "Cluster-based cooperative back propagation network approach for intrusion detection in MANET," in *IEEE 10th International Conference on Computer an Information Technology (CIT'10)*, pp. 1627–1632, 2010.

[21] S. Sujatha, P. Vivekanandan, and A. Kannan, "Fuzzy logic controller based intrusion handling system for mobile ad hoc networks," *Asian Journal of Information Technology*, vol. 7, pp. 175–182, 2008.

[22] M. Y. Tabari, H. Hassanpour, and A. Movaghar, "Proposing a distributed model for intrusion detection in mobile ad-hoc network using neural fuzzy interface," in *Journal of Advances in Computer Research*, vol. 1, pp. 85–96, 2011.

[23] M. Wahengbam and N. Marchang, "Intrusion detection in manet using fuzzy logic," in *3rd IEEE National Conference on Emerging Trends and Applications in Computer Science (NCETACS'12)*, pp. 189–192, 2012.

[24] R. Yager and D. Filev, "Generation of fuzzy rules by mountain clustering," *Journal of Intelligent and Fuzzy Systems*, vol. 2, no. 3, pp. 209–219, 1994.

[25] L. A. Zadeh, "Roles of soft computing and fuzzy logic in the conception, design and deployment of information/intelligent systems," in *Computational Intelligence: Soft Computing and Fuzzy-Neuro Integration with Applications*, NATO ASI, vol. 162, pp. 1-9, Springer, 1998.

[26] Y. Zhang and W. Lee, "Intrusion detection in wireless ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00)*, pp. 275–283, 2000.

Alka Chaudhary received her M.C.A. degree from Institute of Technology and Science (ITS), Mohan Nagar, Ghaziabad in 2010. Currently, she is pursuing Ph.D (Full Time) in Computer Science from Manipal University Jaipur (MUJ), Rajasthan. Her research interests include information security, Mobile Ad Hoc Networks, Neural network, Fuzzy Logic, intrusion detection/prevention, and Network Security.

V. N. Tiwari received his Ph.D degree from IIT, BHU, Varanasi in 1997. He is Currently Working as a HOD of Electronic and Communication Department in Manipal University Jaipur (MUJ), Rajasthan. He has published more than 35 research papers in National/International Journals and Conferences. He has 20 years of R and D and Teaching Experience. His research interests include Microwave Technology, Antennas and Radar.

Anil Kumar received his Ph.D. degree in Computer Science from Sikkim Manipal University, Sikkim (India). He is currently working as a Professor in Department of CSE, Manipal University Jaipur (MUJ). He is an IEEE Senior Member and he is currently guiding 3 - Full Time and 3 - Part Time Research Scholars. His research interests include Image processing algorithm, Cryptography, Artificial Intelligence, Signal and System, Neural System and Genetic Algorithm. He has published more than 70 research papers in international journal and conferences.