# Design an anomaly-based intrusion detection system using soft computing for mobile ad hoc networks

Alka Chaudhary*, V.N. Tiwari and Anil Kumar

Manipal University Jaipur, India
Dehmi Kalan, Near GVK Toll Plaza,
Jaipur-Ajmer Express Highway,
Jaipur, Rajasthan 303007, India
Email: alka.chaudhary0207@gmail.com
Email: vivekanand.tiwari@jaipur.manipal.edu
Email: dahiyaanil@yahoo.com
*Corresponding author

**Abstract:** The main objective of an intrusion detection system is to classify the normal and suspicious activities in the network. The complex characteristics of mobile ad hoc networks make intrusion detection more difficult than for conventional networks. Although, soft computing techniques-based intrusion detection systems proved their effectiveness on wired networks in terms of detecting known and unknown attacks but use of soft computing techniques for mobile ad hoc networks still very restricted so that in this paper, a new scheme has been proposed by using neuro-fuzzy classifier in binary form for mobile ad hoc networks to identify the behaviour of current activities, i.e., normal or abnormal. Qualnet simulator and MATLAB toolbox are used to visualise the attack-based scenarios and evaluate the performance of proposed approach. Simulation results show that the proposed soft computing-based approach is able to identify the known and unknown attacks in mobile ad hoc networks with high positive and low false positive rates.

**Keywords:** mobile ad hoc networks; MANETs; security issues, intrusion detection system; IDS; soft computing; adaptive neuro fuzzy inference system; ANFIS; neuro-fuzzy.

**Reference** to this paper should be made as follows: Chaudhary, A., Tiwari, V.N. and Kumar, A. (2016) 'Design an anomaly-based intrusion detection system using soft computing for mobile ad hoc networks', *Int. J. Soft Computing and Networking*, Vol. 1, No. 1, pp.17–34.

**Biographical notes:** Alka Chaudhary received her MCA degree from Institute of Technology and Science (ITS), Mohan Nagar, Ghaziabad in 2010. Currently, she is pursuing her PhD (Full Time) in Computer Science from Manipal University Jaipur (MUJ), Rajasthan. She has published 12 research papers in international journals and conferences. 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 PhD 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&D and teaching experience. His research interests include microwave technology, antennas and radar.

Anil Kumar received his PhD 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 three full time and three 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 journals and conferences.

## 1 Introduction

Nowadays, mobile ad hoc networks (MANETs) are very attractive in terms of its flexibility during the communication because MANETs do not have any predefined infrastructure or any centralised management points. In MANETs, each mobile node acts as a router as well as mobile node to transmit the data packets across the network. This capability of MANETs makes it more desirable for many applications such as disaster relief management where the disaster relief teams cannot believe in pre-existing infrastructure, military areas where rapidly deployable topology of the network is required in battle fields, communications among groups of people in virtual conferences and neighbourhood area networks and likewise in many other promising areas.

Likewise wired networks, MANETs also face the vulnerabilities against security attacks such as spoofing and are also prone to other types of attacks because of communication via wireless links, resource constraints (bandwidth and battery power), cooperativeness between the mobile nodes and dynamic topology (Li and Wei, 2004).

This paper concentrates on very specific attacks such as sleep deprivation attack and packet dropping attack (PDA) which can easily disrupt the MANETs operations. For the security point of view, prevention-based techniques such as authentication and encryption are not good solutions for MANETs to eliminate the compromised nodes. Hence, intrusion detection system (IDS) is an essential component of security for MANETs so that it is known as the second line of defence for any survivable network security.

When any set of actions attempts to compromise with the security attributes such as confidentiality, repudiation, integrity, and availability of resources then these actions said to be the intrusions and detection of such intrusions are known as IDS (Chaudhary et al., 2014b). The main aim is to classify the intrusive and normal activities in the network. Some detection methods for intrusion detection are presented in literature such as anomaly-based, misuse-based and specification-based methods (Zhang and Lee, 2000).

Many IDSs have been proposed for wired networks in literature but these IDSs could not be directly applied on MANETs due to its specific features, i.e., limited bandwidth, mobility, lack of centralised authority and resource constraint nodes. Consequently, many researchers have been proposed new IDSs for MANETs (Sen and Clark, 2009b). This paper explores the use of soft computing techniques in MANETs. Soft computing is a modern approach towards intelligent systems that are able to handle the imprecision, uncertainty. It is inspired by the human mind (Zadeh, 1998).

In soft computing approaches, fuzzy logic is a robust method that has been proved its applicability in IDSs (Dickerson et al., 2001; Wahengbam and Marchang, 2012). Most of fuzzy systems make their fuzzy rule base on the bases of human expert knowledge that

are lacking of adaptation. Furthermore, fuzzy systems based on adaptation and learning capabilities have found more attention for intrusion detection in networks (Abadeh et al., 2005). Without using human expert knowledge, various methods have been proposed for the automatic formation of fuzzy rules for fuzzy systems, i.e., neuro-fuzzy and fuzzy-genetic (Abadeh et al., 2005; Nauck and Kruse, 1995).

Recently, many of researchers are concentrating on soft computing approaches for the field of intrusion detection in MANETs. Few soft computing techniques were used for detection of intrusions in MANETs (Mitrokosta et al., 2007; Shao et al., 2010; Moradi et al., 2011; Watkins, 2005; Sujatha et al., 2008; Sen and Clark, 2009a). Here, a new scheme designed based on neuro-fuzzy classifier, which is in binary form to distinguish the normal and abnormal activities. For this purpose, adaptive neuro fuzzy inference system (ANFIS) is used as a fuzzy classifier in binary form and, rules are decided by subtractive clustering. The proposed approach works as an anomaly detector for new attacks.

The subsequent sections are as follows: In Section 2, the detailed review of related work. Section 3 defines the working of AODV and presented the target attacks. Section 4 elaborates the soft computing concepts particularly ANFIS, also describe the subtractive clustering technique. In Section 5, the data extraction on specific features has been done with the help of Qualnet simulator 6.1. Sections 6 and 7 explain the proposed system and evaluate the performance of system in distributed environment and Section 8 presents the conclusion.

## 2 Related work

Many soft computing-based IDS systems are employed in wired networks because of their generalised properties that can help to detect known and unknown intrusions or even those attacks that have no prior described patterns (Mukkamala et al., 2005).

Abraham and Jain (2005) illustrated the use of soft computing techniques for building the IDS in wired networks. Neuro-fuzzy classifiers in the form of binary and multi classifiers are applied on intrusion detection to classify the intrusive and normal activities in wired networks by Toosi and Kahani (2007).

Recently, there are few proposed IDSs based on soft computing approaches in MANETs. First, support vector machine-based approach applied in Deng et al. (2003) for intrusion detection in MANETs to emphasise on the security issues of network layer but they are not providing any security mechanism for cluster heads. Some artificial neural network approaches used for MANETs in Mitrokosta et al. (2007), Shao et al. (2010) and Moradi et al. (2011). These proposed neural-based approaches used limited features to detect all possible unknown attacks. Wahengbam and Marchang (2012) suggested fuzzy logic-based IDS for MANETs that is able to detect black hole and gray hole attacks according to the threshold values of each node. In terms of hybrid approaches of soft computing, in Moradi and Teshnehlab (2011), and Yadollahzadeh et al. (2011) used ANFIS as neuro-fuzzy interface with limited features for detection of specific attacks and they were not using any clustering algorithm to automatically generate the initial fuzzy rules and antecedent membership functions without the need of human expert knowledge. The output of these proposed IDSs (Moradi and Teshnehlab, 2011; Yadollahzadeh et al.,

2011) have not mentioned clearly in the form of current data pattern is normal or an attack pattern.

To conclude, we develop a new IDS based on ANFIS as binary neuro-fuzzy classifier with subtracting clustering to automatic generate the initial fuzzy rules and membership functions for MANETs. The proposed system can also detect the new or unknown attacks in MANETs.

## 3 AODV and targeted attacks

In MANETs, one of very commonly used routing protocol is ad hoc on demand distance vector (AODV) (Perkins and Royer, 1999). As an exemplar, AODV protocol is used in this research. This section discussed attacks on AODV that is considered in this research. A detailed description of threats on MANETs is given in Sen et al. (2010).

### *3.1 Packet dropping attack*

In PDA scenario, malicious nodes drop all the incoming data packets for disrupting the network services (Sen et al., 2010). For dropping the data packets, malicious nodes need to be a part of routing path so malicious nodes have little reason to drop control packets such as RREQ, RREP and RERR that are used in route discovery and route maintenance phases of AODV. In this research, control packets are not dropped by the malicious nodes.

Dropping data packets can be prevented the end to end communication between the mobile nodes and also reduced the network performance due to the retransmission of data packets or discovery of new routes. During the simulation of PDA, malicious nodes continuously drop the data packets at each 1 sec interval. As in MANETs, mobility is the major cause to lose the data packet on AODV (Lu et al., 2003). That is why this research concentrates to differentiate the packet dropping due to the mobility from the packet dropping due to malicious nodes in MANETs.

### *3.2 Sleep deprivation attack through malicious RREQ flooding (SDMF)*

The sleep deprivation attack (Pirrete and Brooks, 2006) is a kind of denial of service attack. During this attack, in the route discovery phase of AODV an attacker node broadcasts the route request (RREQ) packets to their neighbour with a destination IP address that exists in the network address range but is actually not present in network. Thus, all presented nodes in the network will compel to forward these RREQ packets because no one is having the route for this fake destination address in the network. The main aim of SDMF attack is to consume the battery power of nodes and discard them to perform the network operations.

Here, SDMF is used in training, checking and testing and PDA is used only in the testing phase, which will be treated as an unknown attack during testing.

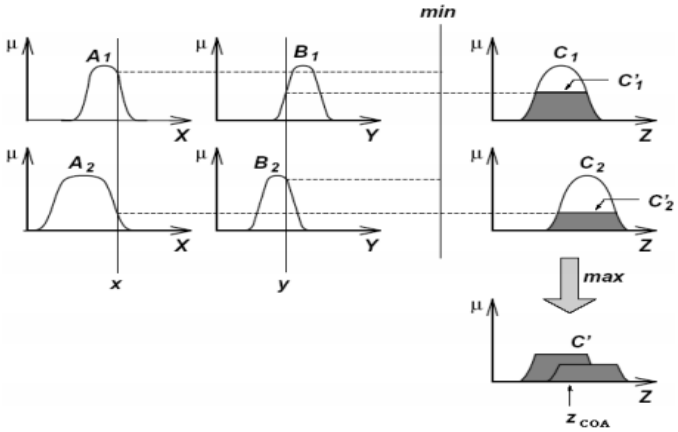
## 4 Fuzzy and neuro-fuzzy

### *4.1 Fuzzy inference system*

Fuzzy logic can easily handle the impreciseness and uncertainty derived from human reasoning. It is able to deal with the multivalued logic of fuzzy set theory within the range 0 to 1. Fuzzy logic-based decisions are in the form of degrees instead of yes or no conditions (Wahengbam and Marchang, 2012). IF-then-else-based fuzzy rules are used to define all situations in the network to identify the attacks or intrusions. The fuzzy rule-based system is known as FIS that is responsible to take decisions based on fuzzy reasoning. Some well-known types of fuzzy inference systems (FISs) have been proposed in the literature (Jang et al., 1997).

At first, two-input single output-based Mamdani FIS proposed to map an input space to an output space which is shown in Figure 1.

**Figure 1** The Mamdani fuzzy interference system with min and max operators




*Source:* Jang et al. (1997)

T-norm and T-conorm operators are choice for max and min. For more acquaintance of T-norm and T-conorm and Mamdani FIS the readers may refer to Jang et al. (1997). Mamdani FIS used defuzzification module that converts the fuzzy values to crisp values in term of output.

There is an example of a Mamdani FIS based on two rules that can be given as

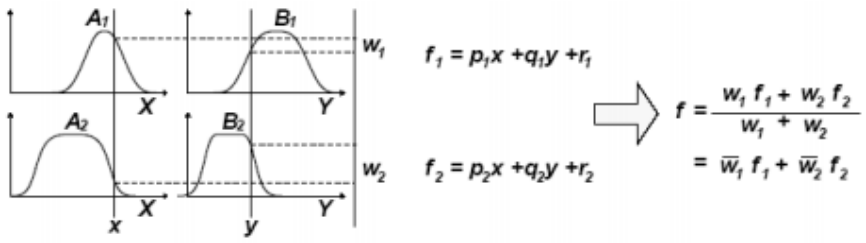
if x is A1 and y is B1 then z is C1,

if x is A2 and y is B2 then z is C2,

where A1, A2 and B1, B2 are the membership functions of inputs for A and B fuzzy sets, and C is the fuzzy sets for output, respectively (Jang et al., 1997).

Takagi, Sugeno, and Kang proposed an approach to generate fuzzy rules from input output dataset (Jang et al., 1997). Two-input and single output-based first order of the fuzzy Sugeno inference system is shown in Figure 2(a).

**Figure 2(a)** Fuzzy reasoning of Sugeno model




*Source:* Jang et al. (1997)

Sugeno model is more efficient towards computation and also more suitable with adaptive techniques. There is an example of a fuzzy rule in Sugeno FIS has the form

if x is A and y is B, then z = f (x, y)

where A and B are the inputs fuzzy sets, and z = f (x, y) is zero or first order polynomial function for crisp output respectively. Here, due to the time consuming procedure of defuzzification in Mamdani fuzzy model is replaced by procedure of weighted average. There are various hybrids of soft computing techniques, where hybrid of fuzzy and neural is very popular in many applications so that Jang et al. (1997) developed a very popular method, which is called ANFIS.

## *4.2 ANFIS*

Whenever, there are some modelling situations in which no one cannot observe and distinguish the membership and the parameters associated with membership for the huge dataset. In this situation, a neuro adaptive learning approach which is integrated in ANFIS can be help.

Adaptive neuro-FIS suggests a method for fuzzy modelling procedure in respect to learn information from a dataset to compute the membership function parameters that allow the related FIS to track in the best way of given input/output data. The parameters related to membership functions will change according to the learning process. For the estimation of membership function parameters, ANFIS can use either back propagation or a combination of back propagation algorithm and least square estimation.

Suppose there is a FIS with two-input x, y single output z to the first order of the Sugeno fuzzy model shown in Figure 2(a). Fuzzy rule set with two fuzzy rules can be given as follows:

if x is A1 and y is B1, then z1 = p1x + q1y + r1,

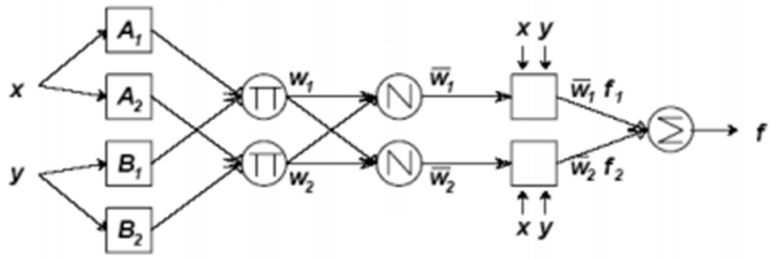
if x is A2 and y is B2, then z2 = p2x + q2y + r2,

The reasoning mechanism of Sugeno model can be applied into a feed forward neural network with the capability of supervised learning, leading so called ANFIS architecture it is shown in Figure 2(b).

In ANFIS architecture, square and circle nodes use as adaptive nodes with parameters and fixed nodes without parameter. Square nodes consist in first layer that perform fuzzification procedure with chosen membership function and the parameters of this layer is known as premise parameters. To produce the firing strength of each rule, t-norm

operations are performed in the second layer. In third layer, calculates the ratio of $i^{th}$ rule firing strength to sum of all rules firing strength for generating the normalised firing strengths. In fourth layer square nodes performed the multiplication of normalised firing strengths with the corresponding rules and the parameters in this layer are called the consequent parameters. The overall output based on the sum of all incoming signals is calculated in fifth layer. For more detail, readers may refer to Jang et al. (1997).

**Figure 2(b)** Structure of ANFIS




*Source:* Jang et al. (1997)

## *4.3 Subtractive clustering*

This paper used the subtractive clustering to find out the initial number of fuzzy rules, membership functions and then ANFIS are used for further fine tuning of functions. ANFIS learning works as similar to the neural networks.

Subtractive clustering (Chiu, 1994) is quick, one pass algorithm to calculate the number of clusters from a given set of data. This method is an extended version of the mountain clustering method that is proposed by Yager and Filev (1994).

Suppose a group of m data points $\{x_1, \ldots, x_m\}$ in N-dimensional points. In subtractive clustering, first assumes all the data points are a potential cluster centre and then measure the potential for each data point of clusters depends on density of surrounding data points. The density of data point $x_j$ can be measured as follows:

$$D_j = \sum_{i=0}^{m} \exp\left(1 - \frac{\left|x_j - x_i\right|^2}{\left(r_a/2\right)^2}\right) \tag{1}$$

where $r_a$ is constant and defines the neighbourhood radius. For the first cluster centre, subtractive algorithm selects the higher density-based data point and then destroys the nearest potential data points of first cluster centre. For the next cluster centre, the algorithm selects the remaining highest density-based data points. The process of evolving a new cluster centre and destroying nearest potential surrounding points of selected cluster centre, repeats this procedure until the potential of all data point fall down a threshold. The influence range of the cluster centre in all data dimensions is known as the cluster radius. A small cluster radius is responsible to find the many clusters in data.

According to the cluster information that is received from this algorithm, is used to find out the initial number of rules and membership functions that are responsible to

generate the FIS. In this work, FIS structure is obtained by the help of subtractive clustering to cover the whole features space. For generation the FIS, grid portioning can be used but the generation of fuzzy rules in grid portioning method depends on the membership functions of every input. Furthermore, if there are three membership functions selected for every input within two dimensional spaces than the results in terms of fuzzy rules will be nine rules so that grid portioning method can make use only small no. of MFs for each input and it creates the problem to moderate the large numbers of inputs (Chiu, 1994). So this paper selected the subtractive clustering approach for determining the numbers of fuzzy rules.

## 5 Features selection and dataset

'Features' are the prominent attributes which are used as an input to our proposed system. Features are supplying the dataset to any evolved system for evaluation of the results. The selection of attributes is most important to develop the system fundamentals. Our system has consideration on the degree of expensiveness of features. Table 1 presents our selected features that are maintained at each node in MANETs through the AODV routing protocol. Basically, here main emphasis is to detect all types of attacks so that it allows to concentrate a rich set of features for proven the efficiency of developed IDS. The features are collected based on two categories, i.e., mobility and packet. Mobility-based features such as added neighbours and remove neighbours give the information about the reflection of mobility for each node. Packet-based features include the control packets of the AODV protocol at each time interval. There are some particular features that have signatures of particular attacks, for example detection the route disruption attack is based on the feature 'average hop count'. The data are gathered based on the selected features periodically by each node. Increments in the no. of data packets that are not forwarded by next node may be signs of PDA.

During the data collection, there is no need of communication between the nodes because all selected features are local to each node (Sen and Clark, 2009a). The unusual decrements in the consumed battery power of each node may be signs of sleep deprivation attack that is happened through malicious flooding in the network.

Here, Qualnet simulator 6.1 (QualNet Network Simulator, http://www.scalable-networks.com) is used to extract the dataset based on selected features for evaluating the results of neuro-fuzzy classifier and Table 2 and Table 3 give the details of training and checking, and testing dataset for neuro-fuzzy classifier. In Table 2, distribution between the normal and attacks type of data for training and checking at the simulation time 1,000 sec is shown, and in Table 3, presents the known and unknown attacks type dataset for testing at simulation time 500 sec, new or unknown attack means which are not presented in the training dataset. Table 4 presents the simulation parameters that are used during simulation phase.

**Table 1** The selected features list

| *Features notations* | *Description* |
|---|---|
| Avg_num_hops | Average number of thehop counts of activeroutes by this node |
| num_routes | No. of routes added tothe route cache |
| num_req_initd | No. of RREQ packetsinitiates by this node |
| num_req_receivd | No. of RREQ packetsreceived to this node |
| num_req_recvd_asDest | No. of RREQ packetsreceived as a destinationfor this node |
| num_rep_initd_asDest | No. of RREP packetsinitiated from thedestination by this node |
| num_rep_initd_asIntermde | No. of RREP packetsinitiated from the anintermediate node |
| num_rep_fwrd | No. of RREP packetsforwarded byintermediate nodes |
| Num_rep_recvd | No. of RREP packetsreceived by this node |
| Num_rep_recvd_asSrce | No. of RREP packetsreceived as source bythis node |
| num_err_initd | No. of RERR packetsinitiated as this nodedetect the link break |
| num_err_fwrd | No. of RERR packetsforwarded by this node |
| num_err_recvd | No. of RERR packetsreceived by this node |
| num_dataPks_Initd | No. of data packets sentas source of the data bythis node |
| num_dataPks_fwrd | No. of data packetsforwarded by this node |
| num_dataPks_recvd | No. of data packets sentas destination of the databy this node |
| Num_brknLinks | Total no. of broken links |
| Consumed_battery | Calculates theconsumed battry toperform any operationby this node |
| Dropped_datapkts | Calculates not forwardeddata packets by this nextnode |

**Table 2** Distribution of data samples in training and checking phase

| *Distributions of data samples* | *Classes* | |
|---|---|---|
| | *Normal* | *Attack (SDMF)* |
| Training | 25,000 | 25,000 |
| Checking | 4,700 | 4,700 |
| Total | 29,700 | 29,700 |

**Table 3** Distribution of data samples in testing phase

| *Distributions of data samples* | *Testing phase* |
|---|---|
| Normal | 9,811 |
| Known attack (SDMF) | 9,800 |
| Unknown attack (PDA) | 9,100 |

**Table 4** Details of selected parameters during simulation

| *Simulation parameters* | |
|---|---|
| Mac type | IEEE 802.11 |
| Simulator | Qualnet 6.1 |
| Routing protocol | AODV |
| Antenna | Omni directional |
| No. of channels | One |
| Channel frequency | 2.4 GHz |
| Packet size | 512 bytes |
| Radio type | 802.11b |
| Energy model | Generic |
| Path loss model | Two ray |
| Pause time | 30 second |
| Battery model | Linear model |
| Simulation time | 1,000 s (training) and 500 s (testing) |
| Batter charge monitoring | Interval 60 Sec. |
| Traffic type | CBR |
| Simulation area | 1,500 m × 1,500 m |
| Number of nodes | 15 and 30 nodes |
| Mobility | Random way point |
| Mobility speeds | 0 to 25 mps |
| Malicious nodes | 4 |

## 6 Proposed architecture

This section explains the proposed architecture of binary neuro-fuzzy classifier-based IDS for MANETs which includes three modules such as data source, detection module, and response module. Figure 3 presents the proposed architecture.

The proposed IDS can detect the attacks in a distributed manner from each node. We used the feature list mentioned in Table 1, as the inputs for binary neuro-fuzzy classifier.

For the point of view binary classifier, patterns are labelled with 0 and 1 where 0 for normal data patterns and 1 for attack data patterns in MANETs. For training and checking, we have used normal and abnormal data as shown in Table 2. For testing, we have used normal, known attack data, i.e., SDMF and, PDA data which are not used in the training phase presented in Table 3.

Here, a subtractive clustering approach used with neighbourhood radius $r_a = 0.5$ to segment the training data and constructs the automatic fuzzy rules to form the structure of FIS for training of ANFIS. The description of subtractive clustering has been presented in Section 4.3.

**Figure 3** Block diagram of proposed system architecture

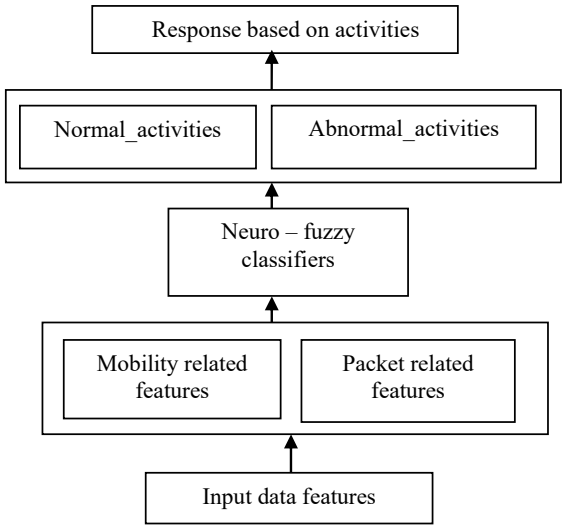
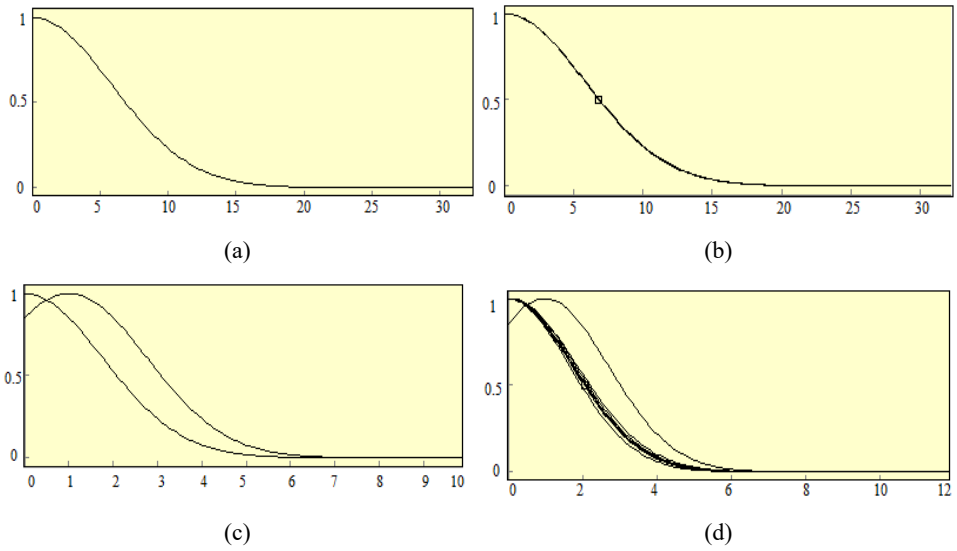



**Figure 4** [(a) and (c)] Initial membership function, i.e., before training and, [(b) and (d)' final membership function, i.e., after training (see online version for colours)




Notes: (a) Before training MFs on input feature 17 (b) After training MFs on input feature 17 (c) Before training MFs on input feature 10 (d) After training MFs on input feature 10

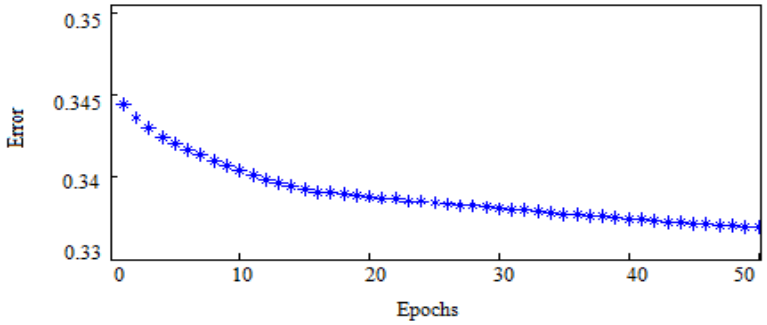
Hence, eight fuzzy rules and eight membership functions (Gaussian type) were obtained for every input. Further fine tuning is done by using ANFIS, training dataset is applied to train the ANFIS and checking dataset is used for validation. Figure 4 shows the initial and final membership functions for some input features during ANFIS training phase. For

model validation checking data are used because after a certain time in the training phase, the model starts overfitting with training dataset. If overfitting occurs then the FIS may behave biased with other independent datasets.

Here, the used ANFIS contains 308 nodes and total numbers of fitting parameters are 416, in which premise parameters are 272 and consequent parameters are 144.

After learning for 50 epochs, the root mean square error (RMSE) for training is 0.3368 and checking is 0.3618, respectively. Figure 5 presents the RMSE error measures as a function based on epochs during the training phase. ANFIS architecture gives only one output that has been previously mentioned in Section 4.2 so in this paper output of ANFIS architecture is specified by the class number, where class number 0 denotes the normal activities and 1 denotes the attacks.

**Figure 5** Represents RMSE error and epoch numbers during training phase (see online version for colours)




The output of ANFIS is not necessary to give output in terms of integer class number, i.e., 0 or 1 So that it needs to be approximated class number with the help of rounding off the given number.

For this reason, μ is a parameter for responsible to the rounding off and provides the integer value to us. If it is given 1 then the specified pattern is attack otherwise it should be normal. Below, we will show the effect of μ on the bases of performance metrics.

For the performance evaluation of an IDS, some standard matrices were developed, i.e., the true positive rate and false positive rate (Sen and Clark, 2009b). True positive rate is calculated by the ratio between the number of truly detected attacks and numbers of total attacks presented in the network and false positive rate can be calculated as the ratio between the numbers of nodes with legitimate behaviour detected attacks and total number of nodes with legitimate behaviour.

## 7 Results analysis

From the results point of view, two different ways of testing have been employed to analyse the performance of our proposed IDS. In first way of testing, we used all the patterns with correctly labelled dataset to test our IDS. In another way, the test dataset has unknown attack which were not a part of the training dataset. So for this purpose, SDMF is used as a known attack and PDA is used as an unknown attack to test the system.

**Table 5(a)** True positive rate and false positive rate of network size 15 during testing at μ = 0.5

| *No. of nodes* | *Traffic* | *Mobility* | *Sleep deprivation attack (SDMF)* | | *Packet dropping attack (PDA)* | |
|---|---|---|---|---|---|---|
| | | | *True positive rate* | *False positive rate* | *True positive rate* | *False positive rate* |
| 15 | Low | Low | 99.11% | 0.85% | 98.55% | 1.60% |
| 15 | Low | medium | 99.83% | 0.63% | 98.21% | 1.53% |
| 15 | Low | high | 99.77% | 1.32% | 99.21% | 2.30% |
| 15 | Medium | low | 99.27% | 1.87% | 98.11% | 2.54% |
| 15 | Medium | medium | 99.42% | 2.10% | 98.74% | 2.97% |
| 15 | Medium | high | 98.30% | 1.92% | 96.99% | 3.05% |
| 15 | High | low | 99.21% | 1.02% | 97.51% | 1.32% |
| 15 | High | medium | 99.32% | 2.31% | 98.54% | 3.77% |
| 15 | High | high | 98.96% | 3.24% | 96.22% | 4.81% |

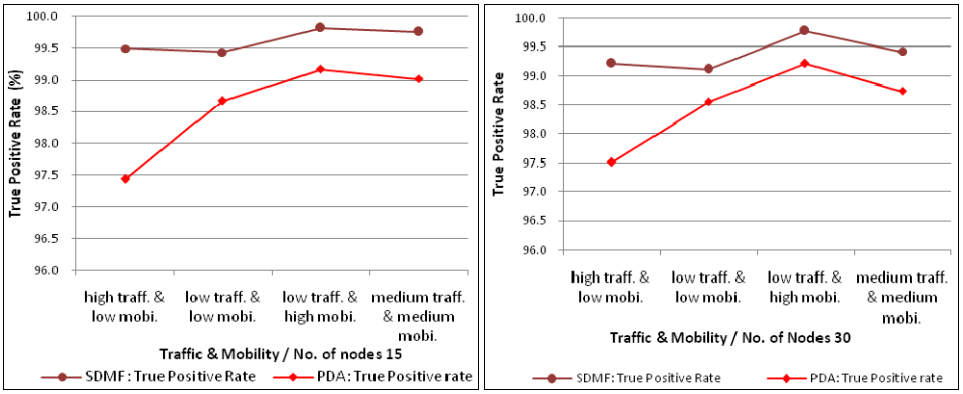
**Table 5(b)** True positive rate and false positive rate of network size 30 during testing at μ = 0.5

| *No. of nodes* | *Traffic* | *Mobility* | *Sleep depriviation attack (SDMF)* | | *Packet dropping attack (PDA)* | |
|---|---|---|---|---|---|---|
| | | | *True positive rate* | *False positive rate* | *True positive rate* | *False positive rate* |
| 30 | Low | Low | 99.43% | 0.99% | 98.67% | 1.87% |
| 30 | Low | Medium | 99.85% | 0.76% | 98. 32% | 1.82% |
| 30 | Low | High | 99.81% | 1.33% | 99.17% | 3.11% |
| 30 | Medium | Low | 99.34% | 1.77% | 98.21% | 2.76% |
| 30 | Medium | Medium | 99.75% | 2.22% | 99.02% | 3.51% |
| 30 | Medium | High | 98.64% | 2.10% | 96.67% | 3.51% |
| 30 | High | Low | 99.49% | 1.23% | 97.44% | 1.93% |
| 30 | High | Medium | 99.46% | 2.37% | 98.11% | 4.11% |
| 30 | High | High | 98.32% | 3.74% | 96.58% | 5.52% |

The test result of our classifier is demonstrated in Tables 5(a) and 5(b). The test results presented the best performance with high true positive rate and low false positive rate in respect of low, medium and high levels of mobility and traffic patterns with varying network size. Figures 6(a) and 6(b), and Figures 7(a) and 7(b) presented the true positive rates and false positive rate of sleep deprivation attack (SDMF) and PDA during variation in network size.

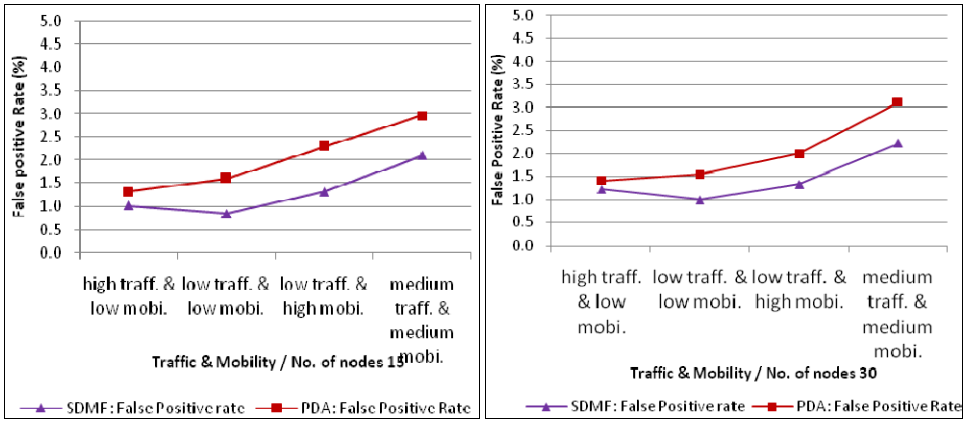
The results show that our proposed IDS can also detect the unknown attacks very efficiently those are not presented in our training dataset.

**Figure 6** (a) True positive rate of SDMF and PDA with network size 15 (b) True positive rate of SDMF and PDA with network size 30 (see online version for colours)




(a) (b)

**Figure 7** (a) False positive rate of SDMF and PDA with network size 15 (b) False positive rate of SDMF and PDA with network size 30 (see online version for colours)



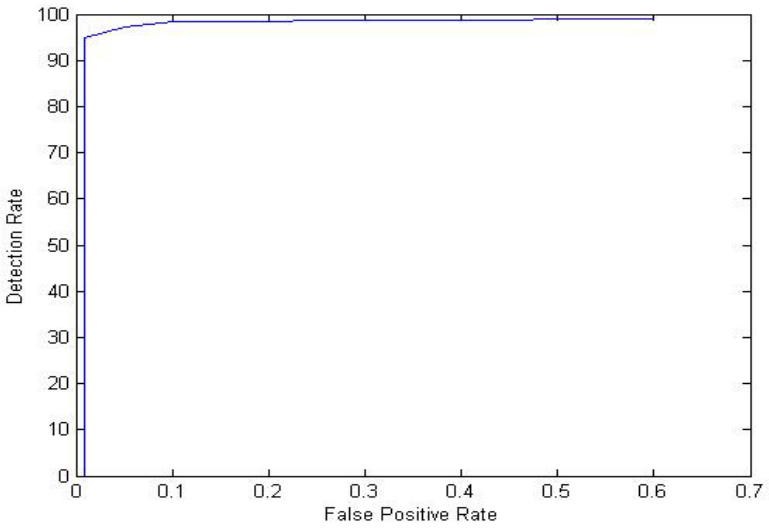

(a) (b)

Table 6 presents the comparison chart of true positive rates (TPR) and false positive rates (FPR) between our proposed neuro-fuzzy classifier and other approaches (Liu et al., 2005; Yadollahzadeh et al., 2011; Shao et al., 2010; Chaudhary et al., 2014a, 2014b) that have been proposed in literature. For this purpose in our way, we setup the same simulation environment in respect of features, training and testing times and no. of malicious nodes that have been considered in comparative techniques (Liu et al., 2005; Yadollahzadeh et al., 2011; Shao et al., 2010; Chaudhary et al., 2014a, 2014b). From the comparison table it is noticed that our classifier performed much better than the other approaches in regards of reducing false positives rate and increasing the true positive rate.

**Table 6** Comparison between our proposed neuro fuzzy classifier and other approaches

| Detection way | Binary-neuro fuzzy classifier with subtractive clustering | Distributed cross-layer intrusion detection system (Liu et al., 2005) |
|---|---|---|
| | *TPR/FPR* | *TPR/FPR* |
| Packet dropping attack | 95.3%/0.43% | 93%/0.5% |
| Sleep deprivation attack | 96.7%/0.62% | 90%/0.7% |
| Detection way | Binary-neuro fuzzy classifier with subtractive clustering | Neuro-fuzzy interface (Yadollahzadeh et al., 2011) |
| | TPR/FPR | TPR/FPR |
| Packet dropping attack | 89%/1.8% | 76%/2.5% |
| Detection way | Binary-neuro fuzzy classifier with subtractive clustering | Cluster-based cooperative back propagation network approach (Shao et al., 2010) |
| | FPR | FPR |
| Packet dropping attack | 5.7% | 7% |
| Detection way | Binary-neuro fuzzy classifier with subtractive clustering | Mamdani fuzzy inference-based approach (Chaudhary et al., 2014a) |
| TPR/FPR | TPR/FPR | |
| Packet dropping attack | 99.4%/0.6% | 98.3%/1.3% |
| Detection way | Binary-neuro fuzzy classifier with subtractive clustering | Sugeno fuzzy inference-based approach (Chaudhary et al., 2014b) |
| | TPR/FPR | TPR/FPR |
| Packet dropping attack | 95.3%/1.1% (under high mobility) | 89.1%/1.6% (under high mobility) |

**Figure 8** Analysis of ROC curve for neuro fuzzy classifier $0 \leq \mu \leq 0.5$ (see online version for colours)



For the performance evaluation of neuro-fuzzy classifier, this paper used the receiver operating characteristics (ROC) analysis in the respect of parameter μ to show the effect on the true positive rate and false positive rate. We changed the value of parameter μ between 0 to 0.5 and then plotted the coordinate point on the bases of (FPR, TPR)μ to see the variation between true positive rate and false positive rate (Gomez and Dasgupta, 2002). Figure 8 displays the ROC curve with respect of μ for neuro-fuzzy classifier which has been used in this paper.

## 8 Conclusions

Here, we have introduced a new IDS based on neuro-fuzzy classifier in binary form for MANETs that is able to detect the attacks from each node in a distributed manner. We used ANFIS as binary neuro-fuzzy classifier so that output of proposed system shows in the form of 0 and 1. This paper applied subtractive clustering technique for specifying the initial fuzzy rules and membership functions without the need of human expert knowledge. The experiment results presented that the evolved fuzzy rules are very efficient to detect the intrusions in MANETs. The results also illustrate that the proposed system is able to detect the unknown attacks. In our future work, we are concentrating to develop the cooperative-based IDS using neuro-fuzzy classifier with more attack simulations and also giving more emphasis on 'which type of attack is detected' in the form of output.

## References

Abadeh, M.S., Habibi, J. and Lucas, C. (2005) 'Intrusion detection using a fuzzy genetics-based learning algorithm', *Journal of Network and Computer Applications*, Vol. 30, No. 1, pp.414–428.

Abraham, A. and Jain, R. (2005) 'Soft computing models for network intrusion detection systems', *Studies in Computational Intelligence*, pp.191–211.

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

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

Chiu, S. (1994) 'Fuzzy model identification based on cluster estimation', *Journal of Intelligent & Fuzzy Systems*, Vol. 2, No. 3, pp.267–278.

Deng, H., Zeng, Q. and. Agrawal, D.P (2003) 'SVM-based intrusion detection system for wireless ad hoc networks', in *VTC'03: Proceedings of the IEEE Vehicular Technology Conference*, Orlando, Florida, USA, pp.2147–2151.

Dickerson, J.E., Juslin, J., Koukousoula, O. and Dickerson, J.A. (2001) 'Fuzzy intrusion detection' in: *Proceeding of IFSA World Congress and 20th North American Fuzzy Information Processing Society (NAFIPS) International Conference*, 25–28 July, Vancouver, Canada, IEEE Computer Society, Vol. 3, pp.1506–1510.

Gomez, J. and Dasgupta, D. (2002) 'Evolving fuzzy classifiers for intrusion detection', in *Proceedings of the 2002 IEEE Workshop on Information Assurance*, New York, Vol. 6, No. 3, pp.321–323.

Jang, J.S.R., Sun, C.T. and Mizutani, E. (1997) *Neuro-Fuzzy and Soft Computing – A computational Approach to Learning and Machine Intelligence*, 1st ed., Prentice Hall, India.

Li, Y. and Wei, J. (2004) 'Guidelines on selecting intrusion detection methods in MANET', in *Proceedings of the Information Systems Education Conference, EDSIG*, pp.1–17.

Liu, Y., Li, Y. and Man, H. (2005) 'Short paper: a distributed cross-layer intrusion detection system for ad hoc networks', in *SecureComm 2005: Proceedings of First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pp.418–420.

Lu, Y., Zhong, Y. and Bhargava, B. (2003) *Packet Loss in Mobile Ad Hoc Networks*, TR 03–009, Dept. of Computer Science, Purdue University.

Mitrokosta, A., Komninos, N. and Douligeris, C. (2007) 'Intrusion detection with neural networks and watermarking techniques for MANETs', in *Proceedings IEEE International Conference on Pervasive Services*, pp.118–127.

Moradi, Z. and Teshnehlab, M. (2011) 'Intrusion detection model in MANETs using ANNs and ANFIS', in *2011 International Conference on Telecommunication Technology and Applications Proc. of CSIT*, Vol. 5.

Moradi, Z., Teshnehlab, M. and Rahmani, A.M. (2011) 'Implementation of neural networks for intrusion detection in MANET', in *ICETECT 2011: Proceedings International Conference on Emerging Trends in Electrical and Computer Technology*, pp.1102–1106.

Mukkamala, S., Sung, A.H. and Abraham, A. (2005) 'Intrusion detection using an ensemble of intelligent paradigms', *Journal of Network and Computer Applications*, Vol. 28, No. 2, pp.167–182.

Nauck, D. and Kruse, R. (1995) 'NEFCLASS – a neuro-fuzzy approach for the classification of data', in *Proceeding of 1995 ACM Symposium on Applied Computing*, Nashville, USA, ACM Press, New York, pp.461–465.

Perkins, C. and Royer, E. (1999) 'Ad-hoc on-demand distance vector routing', in *Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications*, IEEE, pp.90–100.

Pirrete, M. and Brooks, R. (2006) '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.

QualNet Network Simulator [online] http://www.scalable-networks.com (accessed 16 September 2013).

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

Sen, S. and Clark, J.A. (2009b) 'Intrusion detection in mobile ad hoc networks', *Guide to Wireless Ad Hoc Networks*, Chapter 17, pp.427–454, Springer, London.

Sen, S., Clark, J.A. and Tapiador, J.E. (2010) 'Security threats in mobile ad hoc networks', *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, Auerbach Publications, pp.127–147.

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

Sujatha, S., Vivekanandan, P., Yogesh, P. and Kannan, A. (2008) 'Fuzzy logic controller based intrusion handling system for mobile ad-hoc networks', *Asian Journal of Information Technology*, pp.175–182.

Toosi, A.N. and Kahani, M. (2007) 'A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers', *Computer Communication*, Vol. 30, No. 10, pp.2201–2212.

Wahengbam, M. and Marchang, N. (2012) 'Intrusion detection in MANET using fuzzy logic', in *NCETACS 2012: Proceedings of the 3rd IEEE National Conference on Emerging Trends and Applications in Computer Science*, pp.189–192.

Watkins, D. (2005) 'Tactical MANET attack detection based on fuzzy sets using agent communication', in *Proceedings 24th Army Science Conference*, Orlando, FL.

Yadollahzadeh, T.M., Hassanpour, H. and Movaghar, A. (2011) 'Proposing a distributed model for intrusion detection in mobile ad-hoc network using neural fuzzy interface', *Journal of Advances in Computer Research*, Vol. 2, No. 2, pp.1–109.

Yager, R. and Filev, D. (1994) 'Generation of fuzzy rules by mountain clustering', *Journal of Intelligent & Fuzzy Systems*, Vol. 2, No. 3, pp.209–219.

Zadeh, L.A. (1998) 'Roles of soft computing and fuzzy logic in the conception, design and deployment of information/intelligent systems', *Computational Intelligence: Soft Computing and Fuzzy-Neuro Integration with Applications*, Springer, Berlin, Heidelberg, pp.1–9.

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