International Journal of Computing and Applications | **ISSN: 0973-5704**
Volume 13, Number 2, (July-December 2018), pp 355-360
© Serials Publications, New Delhi (India)

SOFT COMPUTING TECHNIQUES FOR INTRUSION DETECTION IN MOBILE AD HOC NETWORKS

Alka Chaudhary[1]

[1] *Assistant Professor, Dept. of IT, Manipal University Jaipur, Jaipur, India. Email: alka.chaudhary@jaipur.manipal.edu*

Abstract: Mobile ad hoc networks (MANETs) are very suitable for communication in the absence of pre-defined infrastructure but it is extremely prone to attacks due to its characteristics such as dynamic topologies, no centralized points and lack of a clear boundary of defense so that detection of intrusions is very difficult in MANETs than the conventional networks. The main intention of intrusion detection system is to classify the normal and abnormal activities. This paper focuses to develop local architecture of intrusion detection system based on soft computing approach for classifying the normal and abnormal activities in MANETs The implementation results show that the proposed intrusion detection system is able to detect the known and unknown attacks with high detection rates.

Keywords: Mobile Ad Hoc Networks (MANETs), Intrusion Detection System (IDS), Soft Computing, Neuro-Fuzzy, Fuzzy Inference System (FIS).

1. INTRODUCTION

MANETs are able to form the wireless network of mobile nodes without the relay on fixed infrastructure. One of very trustable system for security of wireless ad hoc networks is intrusion detection system (IDS) [1] [2]. Many detection methods are used in literature i.e. misuse, anomaly and specification. Here, in this paper misuse and anomaly detection methods are used. This paper examines the use of soft computing techniques for MANETs. Hence, a new IDS based on soft computing techniques is proposed for MANETs.

The subsequent sections are as follows: section II, the detailed review of related work. Section III, explain the soft computing concepts particularly fuzzy inference systems, ANFIS, also describe the subtractive clustering technique. Section IV, elaborates the architecture of proposed IDS. Section V, presents the feature selection and dataset. Section VI, define the experimental results of proposed IDS and then finally conclusion is presented in section VII.

2. RELATED WORK

In wired networks, One of very popular soft computing based IDS proposed by Abraham et. al., for wired networks [3][4]. 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 et. al., [5].

Recently, few soft computing techniques have been applied for detection of intrusions in MANETs [6-11]. M. Wahengbam et. al., [12] Marchang suggested fuzzy logic based IDS for MANETs that can able to detect black hole and gray hole attacks according to the threshold values of each node. In respect of hybrids of soft computing based techniques, in [12][13][14] used ANFIS as neuro-fuzzy interface with limited features for detection of specific attacks.

To conclude, we proposed a novel IDS based on soft computing techniques i.e. neuro - fuzzy classifiers and fuzzy inference system to detect the attack type and unknown attacks in MANETs.

You begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination

anywhere in the paper. Do not number text heads-the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

3. SOFT COMPUTING

Soft computing is an advanced approach for handling the uncertainty and imprecision Fuzzy logic can able to handle the uncertainty that is derived from human reasoning. The decisions of fuzzy logic are multi valued logic of fuzzy set theory between the ranges of 0 to 1. In general, fuzzy rule based systems are known as fuzzy inference systems (FISs). Some well-known FISs have been proposed in literature [15]. One of very popular hybrid approach developed by Jang which is called ANFIS [15]. ANFIS suggests a procedure for fuzzy modeling in respect of learning the information from a given dataset for computing the parameters of membership functions that allow the related FIS to track or handle in best way of given input and output data. ANFIS can use back propagation algorithm or aggregation of back propagation algorithm and least square estimation. Figure 1 elaborates the ANFIS architecture.

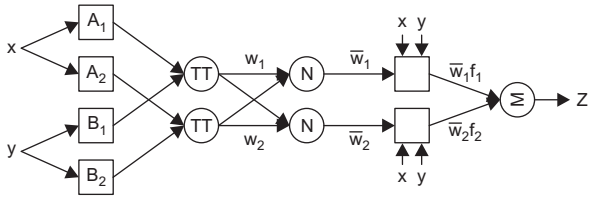

Figure 1: Equivalent ANFIS structure [15]

This paper used the subtractive clustering [16] for automatic formation of fuzzy rules and membership functions.

4. PROPOSED ARCHITECTURE

The proposed IDS based on soft computing techniques is divided into two layers, where first layer consists of the four "ANFIS" blocks and one "Other" block. Each ANFIS block is trained with one of particular type of attack from the dataset. In this research, we have focus on packet dropping attack (PDA), Sleep Deprivation Attack through Malicious Flooding (SDMF) and route disruption attack (RDA). The output of each ANFIS block shows the degree of relatedness of data in terms of each particular attack so that "1" represents the total relationship and "-1" shows otherwise. It must be stated here that ANFIS system provides one output.

Here, subtractive clustering approach used with neighbourhood radius ra = 0.5 for segmentation the training data and constructs the automatic fuzzy rules to form the structure of FIS for training of each ANFIS block. After training of 50 epochs, FIS with minimum checking error has been selected for each ANFIS.

The "Other" block is responsible to store the input data patterns that are not matched with above four "ANFIS" blocks and these input data patterns are treated as an unknown attack patterns that are represented with 1 in terms of output for this block. In second layer, a five input and single output based Mamdani FIS are used to make the decision that the current input data pattern is attack or not. For this purpose, two Gaussian type membership functions are selected for every input fuzzy set and fuzzy rule base for Mamdani FIS is given in Table 1. Here, output of Mamdani FIS depicted between −1 and 1 so that 1 presents the current input pattern is an attack and -1 shows the current input pattern is normal. This paper is emphasized on local IDS architecture i.e. Local IDS that is based on proposed soft computing approach.

In Local IDS, each mobile node is having an IDS agent in the network and detects the attacks on the bases of their own decision. Here, mobile nodes communicate with their neighbour nodes that are only one hop away for making the decisions on malicious activities are presented in the network or not.

5. FEATURES SELECTION AND DATASET

Features are supply as an input dataset to any evolved system for evolution of the results. Table 2 presented 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 concentrates 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 AODV protocol at each time interval. Here, Qualnet simulator 6.1 [17] is used for extracting the dataset based on selected features to evaluate the performance of proposed IDS in respect of each attack category so that Table 3 & 4 are given the details of training and checking data.

6. RESULTS ANALYSIS

In this paper, Local IDS architecture has been implemented based on proposed soft computing approach so that training and testing datasets are presented in Table 3 & 4 at 1000sec and 500 sec simulation time for evaluating the performance of ANFIS classifiers.

Some other new attacks patterns that are not presented in the training data set. The results of proposed IDS is presented in Table 5, 6 & 7.

Table 1
Fuzzy rule base for proposed Mamdani FIS

Normal	*PDA*	*SDMF*	*RDA*	*Others*	*Output*	*Attack Type*
High	--	--	--	--	Normal	Normal
--	High	--	--	--	Attack	PDA Attack
--	--	High	--	--	Attack	SDMF Attack
--	--	--	High	--	Attack	RDA Attack
--	--	--	--	High	Attack	Unknown Attack
--	Low	Low	Low	Low	Normal	Normal
--	!=High	!=High	!=High	!=High	Normal	Normal
Low	--	--	--	--	Attack	Attack (At present time depends on degree of relatedness for which attack block is high)

Table 2
Selected Features

Features	*Explanation*
num_hops	Aggregate sum of the hop counts of all active routes
num_req_recvd_asDest	No. of RREQ packets received as a destination for this node
num_rep_initd_asDest	No. of RREP packets initiated from the destination by this node
num_rep_fwrd	No. of RREP packets forwarded by intermediate nodes
Num_ rep_ recvd	No. of RREP packets received by this node
Num_ rep_ recvd _asSrce	No. of RREP packets received as source by this node
num_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_brknLinks	Total no. of broken links
Consumed_battery	Calculates the consumed battry to perform any operation by this node
Dropped_datapkts	Calculates not forwarded data packets by this next node
num_nbrs	No. of neighbours of node during simulation time
num_addNbrs	No. of added neighbours of node during simulation time
num_rmveNbrs	No. of remove neighbours of node during simulation time

Table 3
Distribution of data samples in training and checking phase for local detection

Data Set for Local Detection					
Distributions of Data Samples		*Normal*	*PDA*	*SDMF*	*RDA*
ANFIS - N	Training	15,000	10,000	12,000	10,000
	Checking	1,500	1,000	12,00	1,200
ANFIS - PDA	Training	10,000	10,000	10,000	10,000
	Checking	1,000	1,000	1,000	1,000
ANFIS - SDMF	Training	6,000	5,000	6,000	5,000
	Checking	1,000	2,500	1,000	1,000
ANFIS - RDA	Training	3,000	5,000	5,000	5,000
	Checking	8,00	2,500	5,00	1,000

Table 4
Distribution of data samples in testing phase for local

Distributions of test Data Samples	*Normal*	*PDA*	*SDMF*	*RDA*
Local Detection	10,000	8,700	9,500	6,000

Table 5
Detection rates of local IDS for packet dropping attack (PDA) with network size 35

No. of Nodes	*Traffic*	*Mobility*	*Packet Dropping Attack (PDA)*	
			Local Detection	
			True Positive Rate	*False Positive Rate*
35	Low	Low	99. 15%	1.35%
35	Low	Medium	99.43%	1.95%
35	Low	High	98.85%	3.22%
35	Medium	Low	99.22%	2.22%
35	Medium	Medium	98.61%	3.46%
35	Medium	High	97.94%	3.78%
35	High	Low	98.53%	3.31%
35	High	Medium	98.03%	4.53%
35	High	High	96.76%	6.12%

Table 6
Detection rates of local IDS for sleep deprivation attack (SDMF) with network size 35

No. of Nodes	*Traffic*	*Mobility*	*Sleep Depriviation Attack (SDMF)*	
			Local Detection	
			True Positive Rate	*False Positive Rate*
35	Low	Low	99.40%	0.86%
35	Low	Medium	99.83%	0.94%
35	Low	High	98.99%	1.23%
35	Medium	Low	99.54%	1.31%
35	Medium	Medium	99.61%	1.79%
35	Medium	High	98.69%	1.85%
35	High	Low	98.32%	1.69%
35	High	Medium	98.55%	2.78%
35	High	High	98.93%	3. 19%

Table 7
Detection rates of local IDS for route disruption attack (RDA) with network size 35

No. of Nodes	*Traffic*	*Mobility*	*Route Disruption Attack (RDA)*	
			Local Detection	
			True Positive Rate	*False Positive Rate*
35	Low	Low	99.11%	0.98%
35	Low	Medium	98.24%	0.72%
35	Low	High	98.77%	0.87%
35	Medium	Low	99.42%	0.99%
35	Medium	Medium	99. 75%	1.16%
35	Medium	High	98.95%	1.59%
35	High	Low	98.88%	1.68%
35	High	Medium	98.84%	2.19%
35	High	High	98.91%	2.99%

7. CONCLUSION

This paper has been introduced a soft computing based IDS for MANETs that can able to make the difference between normal and suspicious activities. Here, ANFIS are used as a neuro-fuzzy classifier and subtractive clustering are selected to automatic forming the fuzzy rules. Finally, the mamdani based fuzzy inference system makes the proposed IDS more capable to detect an attack. Local IDS architecture for MANETs enviourments has been implemented based on proposed soft computing approach. Experiment results are proved that the proposed soft computing approach based IDS are able to detect the both known and unknown attacks with high detection rate. In future, *i* will also develop the distributed and cooperative architecture using soft computing techniques for MANET.

References

[1] Chaudhary, Alka, V.N. Tiwari and Anil Kumar, "A reliable solution against Packet dropping attack due to malicious nodes using fuzzy Logic in MANETs", International Conference on Optimization, Reliability and Information Technology (ICROIT), IEEE, 2014.

[2] Chaudhary, Alka, V.N. Tiwari, and Anil Kumar. "Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks." Advance Computing Conference (IACC), 2014 IEEE International. IEEE, 2014.

[3] S. Sen, J.A. Clark, Intrusion detection in mobile ad hoc networks, in: Guide to Wireless Ad Hoc Networks, Springer, pp. 427-454, 2009.

[4] S. Mukkamala, A.H. Sung, and A. Abraham, "Intrusion detection using an ensemble of intelligent paradigms" Journal of Network and Computer Applications, 28(2):167–182, 2005.

[5] A. Nadjaran Toosi, M. Kahani, R. Monsefi, Intrusion detection based on neuro fuzzy classification, in: Proceedings of IEEE International Conference on Computing and Informatics, 6–8 June 2006, Kuala Lumpur, Malaysia, 2006.

[6] Min-Hua Shao, Ji-Bin Lin; Yi-Ping Lee, "Cluster-based Cooperative Back Propagation Network Approach for Intrusion Detection in MANET in IEEE 10th International Conference on Computer an Information Technology (CIT), 2010.

[7] Zahra Moradi, Mohammad Teshnehlab Amir Masoud Rahmani, " Implementation of Neural Networks for Intrusion Detection in MANET", IN International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT), 2011.

[8] Watkins, Damian. "Tactical manet attack detection based on fuzzy sets using agent communication", In 24th Army Science Conference, Orlando, FL, 2005.

[9] S. Sujatha, P. Vivekanandan, A. Kannan, "Fuzzy logic controller based intrusion handling system for mobile ad hoc networks", Asian Journal of Information Technology, ISSN: 1682- 3915, pp. 175-182, 2008.

[10] S. Sen and J.A. Clark, "A grammatical evolution approach to intrusion detection on mobile ad hoc networks", in Proc. of Second ACM Conference on Wireless Network Security (WiSec'09), 2009.

[11] H. Deng, Q. Zeng, and D.P. Agrawal, "SVM-based Intrusion Detection System for Wireless Ad Hoc Networks", In Proceedings of the IEEE Vehicular Technology Conference (VTC'03), Oct. 2003, Orlando, Florida, USA, pp. 2147-2151.

[12] M. Wahengbam and N. Marchang, "Intrusion detection in manet using fuzzy logic", 3rd IEEE National Conference on Emerging Trends and Applications in Computer Science (NCETACS), ISBN: 978-1-4577-0749-0, pp. 189 – 192, Shillong, 30-31 March 2012.

[13] Moradi, Zahra, and Mohammad Teshnehlab, "Intrusion Detection Model in MANETs using ANNs and ANFIS" , 2011 International Conference on Telecommunication Technology and Applications Proc. of CSIT. Vol. 5. 2011.

[14] Chaudhary, Alka, V.N. Tiwari, and Anil Kumar. "A new intrusion detection system based on soft computing techniques using neuro-fuzzy classifier for packet dropping attack in MANETs." International Journal of Network Security 18.3 (2016): 514-522.

[15] J.S.R. Jang, C.T. Sun and E. Mizutani, "Neuro-Fuzzy and Soft Computing - A computational Approach to Learning and Machine Intelligence", in first edition, Prentice Hall of India, 1997.

[16] S. Chiu, Fuzzy model identification based on cluster estimation, Journal of Intelligent & Fuzzy Systems 2 (3) (1994) 267–278.

[17] QualNet Network Simulator; Available: http://www.scalable-networks.com.