2011 International Conference on Telecommunication Technology and Applications
Proc .of CSIT vol.5 (2011) © (2011) IACSIT Press, Singapore

Intrusion Detection Model in MANETs using ANNs and ANFIS

Zahra Moradi[1], Mohammad Teshnehlab[2]

[1] Parand Branch, Islamic Azad University,Tehran, Iran

[2] K. N. Toosi University of Technology, Tehran, Iran

Abstract. In recent years, different approaches are implemented to improve the security level of Mobile Ad hoc Networks. The aim of this research is to design a mechanism of intrusion detection for this Network to provide a security framework to detect an especial security attack. In a type of attack, considered in this research, an intruder node injects a large amount of junk packets into the network and causes a denial in the services of the attacked node to the network. The model is developed using 2 method of detection – ANFIS and ANNs – in a simulated environment. It is showed that almost all of models can detect Dos attack effectively.

Keywords: Mobile Ad hoc Network, Intrusion Detection, Denial of Service Attack, Artificial neural networks (ANNs), Adaptive Neuro-Fuzzy Inferences System(ANFIS).

1. Introduction

Nowadays, due to expansion of wireless networks and making extensive use of them in scientific, commercial and political communication, providing pertinent field for their operation and function in this kind of networks is of crucial necessity. Along with the growth in computer networks, we are facing with a growing number of attack and intrusion in MANET[3]. Dynamic and unpredictable network topology as well as bandwidth restrictions, energy constraints, high ability in network capacity and its flexibility are among factors facilitating attack against the networks, therefore, it is of prior importance to provide security. In this context various protocols such as SAODV[4], ARAN[5], and SRP[6] have been proposed. In most of them, it is assumed MANET benefits from a secure environment, although, considering the presence of malicious nodes, As a result of open environment, dynamic topology and lake of centralized safety structure, unfortunately these kinds of networks are highly vulnerable [1-2]. Initially, most routing protocols assume that, all network nodes behave in accordance with routing protocols and there are not any malicious nodes these assumptions prepare the way for attacker to network, and therefore, various hidden attacks on routing protocols of these networks can take place [3-4].

2. Related work

Recognizing malicious and selfish nodes is essential to protect the network. As soon as a network is attacked by such nodes its situation will change from a normal to vulnerable state. Malicious nodes posses different behaviour of network compared with normal nodes. For example in some of threat, malicious nodes send unnecessary rout request to all neighbouring nodes and causes flooding packet and its spread throughout the network, leading to energy over-consumption and congestion in the network[5]. One of other misbehaviours is shown by a node is selfishness. Selfish node attempts to reserve its resource by making use of others' services and consuming their resources. Instances issues such as no contribution to routing, lack of broadcasting rout request and packet drop as well as regulating the amount of TTL[7] with the least available

[1] z.moradi@gmail.com

[2] Teshnehlab@eetd.kntu.ac.ir

[3] Mobile Ad hoc Network

[4] Secure Ad hoc on Demand distance Vector

[5] Authenticated Routing for Ad hoc Networks

[6] Secure Routing Protocol

[7] Time To Live

amount, incorporating hop, a change in routing request or routing topology are all considered as malicious behaviour of nodes in the network. Malicious node can be detected by considering such misbehaviour patterns. Sterne *et al.* (2005) Nasser and Chen (2007) have offered intrusion detection and distributed structure, making it possible to detect special attack besides conventional attack to MANET. This structure is designed upon a dynamic hierarchy to detection selfish nodes in MANET. A selfish node attempts to store its resources by using others' which collects data detected from surface, integrate and summarize it. Moreover, it analyzes its movement across the route, and therefore, considers security to management along the route [6-7]. Karg *et al.* (2005) have pointed out ways services and by consuming their resources. They focus on intrusion phase and show different kinds of sensors that could be used to detect selfish nodes [8]. Abraham *et al.* (2006) have stated some of challenges available in designing Intrusion Detection system with high accuracy. They have also shown using of computing intelligence in designing intrusion systems in a distributed environment [9]. Alampalaya and Natsheh (2008) in an article deals with multivariate fuzzy analysis for MANET threat detection. Detection of malicious nodes and selfish nodes is essential to protect MANET and Monitoring mechanisms can collect important network data to detect abnormal behaviours caused by attacks [5]. Makkithaya *et al.* (2008) designed IDS[8] by employing such approaches as data mining and decision tree. In this model they have used fuzzy c-means clustering algorithm. The results show this is an effective way and has better performance than others in intrusion detection system [12]. Kabiri and Zargar (2009) have dealt with clustering and selection of effective parameters in IDS. Due to the fact that IDS parameters may be great in number and employing all them gives rise to computing capacity and complexity of model, therefore they select the most effective parameters. As a result, preparing Intrusion Detection Systems and preventing from attack and intrusion to MANET is of crucial importance [13].

In this paper four essential phases are to be described. These phases include: definition of attack, attack simulation, selecting detection parameters, modelling the process of detecting the nodes under attack. In the first three stages working environment is created by simulation of MANET environment, and in the next stage while, using Neural Networks and Neuro-Fuzzy system, the principal goal of the research, that is Intrusion Detection is applied on the simulated environment.

3. METHODOLOGY

3.1. DOS attack definition

Denial of Service is a kind of conscious and astute attack in which the intruder node disturbs other nodes in the network by sending extra number of packets and causing traffic. This, in turn, leads to restricting resources and imposing over load on data processing to receiver node. Moreover, this node is able to distribute unnecessary or incorrect data in the network so that it can prevent from other nods functioning correctly and in time. Dos attacks are easily created, but they are difficult to detect, hence, they are known as attacks of hackers. In some of DOS attacks, malicious node detects a node with an important role in the network and by keeping it busy in other field rather than its function, causes a vulnerable state in the network. Therefore, we can see that unavailability and disturbance denial of service occurs by under attack node in the network. In some other DOS attacks, through misusing its IP address and creating traffic, some middle nodes are kept busy and therefore prevent them from offering proper service [10].

In this article, the kind of DOS attack is defined in such a way that malicious node disturbs the network by sending large numbers of message packet. This kind of attack is typically illustrated in figure 1. The node A is an under attack node and node C is malicious node in this network. The node C tries to deploy resources of node A by causing heavy traffic and by keeping A busy, prevents it from delivering service to other nodes such as F,E,D,B. as a result, DOS attacks in MANET used to decreasing network performance[5].

[8] Intrusion Detection system

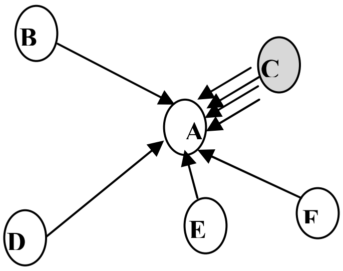

Figure 1. DOS attack, Intruder C bombards the host node A with extra packets.

3.2. Parameter Selection

In general detecting attacks made against the network, is conducted through measuring meaningful parameters and constantly monitoring them. Basically, there are different parameters for any kind of attack depending on their nature and the place where they can affect the network. These parameters can be affected and show their abnormal behaviour. Considering the kind of attack selected in this article, the most important parameters affected by attack, and therefore, can be used in designing Intrusion Detection System includes: Packet drop rate (rate of packets dropping in every second), Delivery rate (rate of packets receiving to their destination correctly in every second), and Buffer capacity using rate (volume of buffer that is filled in every second).

It should be noted that in order to use the above mentioned parameters in detecting under attack node considering the fact that each node may have more than one link with other nodes, and on any link parameters will take different values, thus we should use average value on all links leading to any node, as parameter value for that node. On the other hand it should be born in mind that there is necessarily no need to great number of parameters. Any system which can be designed with fewer parameters but higher detection power will be more useful concerning time and cost.

3.3. Designing Artificial Neural Networks

ANNs are one of the artificial intelligence methods. Designing ANNs is utilized to detect the under attack node. ANN is designed with three inputs; one output includes two middle layers, one input layer and one output layer. This modelling is also carried out with toolbox of MATLAB software. The type of network is selected Feed Forward Back Propagation (FFBP) with training function TARINLM and TARINLM. LEARNGDM is used for adaptive learning function. TANSIG and LOGSIC are selected as Transfer functions also, use declining gradient to train and updating the amount of weights.

3.4. Designing Neuro-Fuzzy System

Modelling system used in this article is Neuro-Fuzzy (Sugeno) as to detect under attack node. Selected parameters from previous stage are given to adaptive Neuro-Fuzzy system. The output of this system shows the state of the node. This research is modelled by toolbox of MATLAB software. This paper is used Hybrid and Back Propagation as learning algorithm. Membership functions are Gaussian and triangle. Furthermore, in order to an increase in accuracy and speed of training process, we normalized the input data and output data at a boundary of [0, 1] into the model.

4. Modeling

4.1. Simulation environment for MANET

Simulation has been carried out by NS2 software. Its purpose is to create MANET and simulation this attack. The details of simulation have been shown in table 1. As it is noticed, in simulated network, AODV routing protocol is used with Mac layer IEEE 802.11. Environment for simulation is selected 500*500 and nodes move randomly between 1 m/s and 10 m/s. The network constructed with 6 nodes that every node is connected at least to one another node via mobile agents. The mobile agents serve as a communication agent between nodes. In the designed network, node number 0 is selected as malicious node and node number 1 as under attack node.

Table1. MANET Configuration in NS2

Parameter	**Definition**
Protocol	Ad hoc on Demand Distance Vector(AODV)
Mac layer	IEEE 802.11
Transmission range	250 m
Node placement	Random
Simulation area	500*500
Minimal speed	1 m/s
Maximal speed	10 m/s
Size of data packets	512 bytes
Traffic sources	Constant Bit Rate (CBR)
Simulation time	300 s
Number of node	6
Version NS-2	NS-2.29(under windows, cygwin)

Using analysis log files of simulation run, the parameters were extracted. 65% of all data (1800 observation including 6 nodes in 300 second) are randomly selected for training data and 15%, 20% for validation and test data respectively.

4.2. Modeling for detection of under attack node by using an Artificial Neuro network

Modelling is done in two stage training and test to detect under attack node from FFBP network, learning algorithm LM, adaptive learning algorithm GDM and two type of transfer function LOGSIC and TANSIG were used under two strategies. Strategy 1 is defined with 15 neurons in the first middle layer and 10 neurons in the second middle layer and in strategy 2 the number of neuron in the first and second middle layer are 20 and 10 respectively. Table 2 illustrated the results of this modelling based on training data. The amount of the best state is shown in grey in the table. At the next stage the accuracy degree of the model was assessed by using test data. The results are reflected in table 3.

Table2. Modeling ANNs based on training data

Network type	Learning algorithm	Adaptive learning algorithm	Number of layers and neurons	Transfer function	R2	RMSE	MAE	Epoch
FFBP	LM	GDM	3-15-10-1	LOGSIG	0.9797	0.1905	0.0746	12
					0.9847	0.1900	0.0725	29
				TANSIG	0.9847	0.0430	0.0035	15
					0.9732	0.0581	0.0124	10
			3-20-10-1	TANSIG	0.9848	0.0430	0.0035	39
					0.9847	0.0743	0.0033	21

Table3. Modeling ANNs based on testing data

Network type	Learning algorithm	Adaptive learning algorithm	Number of layers and neurons	Transfer function	R^2	RMSE	MAE
FFBP	LM	GDM	3−15−10−1	LOGSIC	0.9382	0.1987	0.0815
					0.9388	0.1986	0.0801
				TANSIG	0.9792	0.0519	0.0044
					0.9702	0.0615	0.0137
			3−20−10−1		0.9584	0.0741	0.0072

				TANSIG	0.9582	0.0430	0.0069

4.3. Modeling detection of under attack node by using Neuro-Fuzzy

Modelling is conducted at two training and testing levels. This system was modelled with three input parameters. Table 5 and table 6 shows the results.

Table5. ANFIS model for training data

Epoch	MAE	RMSE	R^2	Number of Membership Function	Membership function	Learning algorithm
100	0.0088	0.0593	0. 9711	3 3 3	Trimf	Back Propagation
100	0.0094	0.0536	0.9766	3 3 3	Gaussmf	
100	0.0068	0.0332	0.9909	3 3 3	Trimf	Hybrid
100	0.0018	0.0292	0.9930	3 3 3	Gaussmf	

Table6. ANFIS model for testing data

MAE	RMSE	R^2	Number of membership Function	Membership function	Learning algorithm
0.0166	0.0976	0.9287	3 3 3	Trimf	Back Propagation
0.0130	0.0747	0.9576	3 3 3	Gaussmf	
0.0142	0.0694	0.9642	3 3 3	Trimf	Hybrid
0.0018	0.0554	0.9767	3 3 3	Gaussmf	

5. Results and discussion

Designed models showed that the main objective of the research namely intrusion detection, was also conducted in a simulated environment to evaluate the models. Three measures by the root mean square error (RMSE), determination coefficient (R2) and absolute error (MAE) were employed. The best result in ANNs for FFBP network with TANSIG function is related to 3-15-10-1 topology that produce RMSE=0.0430, R2 = 0.9847 in 13 epoch. Two figures 2 and 3 show determination coefficient for training and testing models. ANFIS model with hybrid learning algorithm and Gaussian membership function had the best results and allocated itself the highest determination coefficient among other systems (RMSE=0.0292, R2 = 0.9930). Although both models show high rate of detection but the ANFIS model has higher rates.

6. References

[1] Papadimitratos, P. and Haas, Z. J. “Secure Routing for MANETs,” SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 27-31.

[2] Sanzgiri, K.; Dahill, B.; Levine, B. N.; Shields, C. and Belding-Royer, E. M. “A Secure Routing Protocol for Ad Hoc Networks,” in Proceedings IEEE International Conference on Network Protocols (ICNP) , 2002.

[3] Khatib, K. El.; Korba, L.; Song, R.; and Yee, G.; “Secure dynamic distributed routing algorithm for ad hoc wireless networks,” in proceedings of International Conference on Parallel Processing Workshops (ICPPW’03) 2003..

[4] Jakobsson, M. and Wetzel, S.; “Stealth Attacks on Ad-hoc Wireless Networks,” in Proceedings of Vehicular Technology Conference,2003.

[5] Alampalayam Sathish Kumar, Essam F. Natsheh," Multivariate Fuzzy Analysis for Mobile Ad hoc Network Threat Detection", International Journal of Business Data Communications and Networking , Volume 4, Issue 3, 2008.

[6] Nasser, N.; Chen, Y., "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad-hoc Networks," Communications, ICC '07. IEEE International Conference on , vol., no., pp.1154-1159, 24-28, 2007.

[7] Sterne, D.; Balasubramanyam, P.; Carman, D.; Wilson, B.; Talpade, R.; Ko, C.; Balupari, R.; -Y. Tseng, C.;.Bowen, T.; Levitt, K. and Rowe, J. “AGeneral Cooperative Intrusion Detection Architecture for MANETs,”Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA’05), pp. 57-70, 2005.

[8] Kargl Frank, Andreas Klenk, Stefan Schlott, and Michael Weber," Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks", Multimedia Computing, Ulm, Germany, 2005.

[9] Abraham, Ajith, Crina Grosan, Yuehui Chen, " Evolution of Intrusion Detection Systems", School of Information Science and Engineering Jinan University, Jinan 250022, P.R.China, 2006.

[10] Michiardi, P. and Molva, R. "Prevention of denial of service attacks and selfishness in mobile ad hoc networks," Institute Eurecom, Research Report RR-02-063, 2002.

[11] Jang Jyh-S hing Roger ," Input Selection for ANFIS Learning", IEEE 0-7803-3645-3/96, 1996.

[12] Makkithaya Krishnamoorthi, N.V. Subba Reddy, and U. Dinesh Acharya**,** 2008, " Intrusion Detection System using Modified C-Fuzzy Decision Tree Classifier", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.11.

[13] Kabiri, Peyman and Gholam Reza Zargar," Category-Based Selection of Effective Parameters for Intrusion Detection", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.9, 2009.