Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 151 (2019) 1176–1181

Procedia Computer Science

www.elsevier.com/locate/procedia

International Workshop on Web Search and Data Mining (WSDM)
April 29 - May 2, 2019, Leuven, Belgium

Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET

Houda Moudni[a,*], Mohamed Er-rouidi[b], Hicham Mouncif[c], Benachir El Hadadi[a]

[a] *Laboratory of Sustainable Development, Faculty of Sciences and Technology, Sultan Moulay Slimane University, Beni Mellal, Morocco*
[b] *Faculty of Sciences and Technology, Sultan Moulay Slimane University, Beni Mellal, Morocco*
[c] *Faculty Polydisciplinary, Sultan Moulay Slimane University, Beni Mellal, Morocco*

Abstract

Mobile Ad hoc NETworks (MANETs) are a new type of wireless communications that are operating in a highly dynamic and unpredictable environment. These networks are becoming increasingly popular and more essential to wireless communications in recent years due to their ease of deployment and growing popularity of mobile devices. A MANET is a group of wireless mobile nodes that are able to communicate with each other without using centralized administration or fixed infrastructure. Therefore, providing communications even in the absence of any fixed infrastructure or centralized administration, MANETs became an attractive technology for many applications. However, this flexibility brings new threats to security. The black hole attack is considered as one of the most affected kind on MANETs. In addition, the traditional method of protecting wired networks or wireless networks with infrastructure does not apply directly to MANETs. Since prevention techniques are never enough, the use of an Intrusion Detection System (IDS) has a major importance in the MANET protection. In this paper, a new scheme has been proposed by using an Adaptive Neuro Fuzzy Inference System (ANFIS) and Particle Swarm Optimization (PSO) for mobile ad hoc networks to detect the black hole attack.

Keywords: Mobile Ad Hoc Networks; Security; Intrusion Detection System; Black Hole Attack; ANFIS; PSO;

1. Introduction

A decade of exponential growth in wireless networks has profoundly affected our lifestyle, from cell phones to wireless internet access. A wireless network without any fixed infrastructure or centralized administration is called a Mobile Ad hoc NETwork (MANET) [1], since the wireless nodes can move freely. It is a mobile, multi-hop and wireless network that operates without the existing of any fixed infrastructure or centralized administration, except

* Corresponding author. Tel.: +212678530277.
E-mail address: h.moudni@usms.ma

1877-0509
10.1016/j.procs.2019.04.168

for the nodes themselves. These unique characteristics allow to be used in special applications such as the military, disaster relief management, communication between groups of people in virtual conferences and likewise in many other promising areas. Routing in such networks is difficult because the conventional routing protocols do not operate efficiently in the presence of frequent movement, intermittent connectivity, and a dynamic topology. In addition, the use of wireless links makes these networks highly vulnerable to the security attacks, ranging from passive listening to active interference. The black hole attack is considered as the one of the most affected kind on these networks [2],[3]. In order to protect the network from this attack, the use of an Intrusion Detection System (IDS) [4] has a major importance in the MANET protection. In this paper, a new IDS has been proposed by using an Adaptive Neuro Fuzzy Inference System (ANFIS) [5] and Particle Swarm Optimization (PSO) [6] for mobile ad hoc networks to detect the black hole attack.

2. Related research

In recent years, different methods have been proposed in the literature to improve security in MANETs. These methods can be cryptographic solutions [7],[8], modification in the routing protocol mechanism [9] or Intrusion Detections Systems . However, they are mostly focused on detecting and preventing specific attacks. For example, E. VishnuBalan et al. [10] proposed an intrusion detection system to detect and identify the black hole attack and the gray hole attack by using fuzzy logic technique. A. Chaudhary et al. [11] proposed an IDS based on Neuro-fuzzy classifier in binary form for mobile ad hoc networks to identify the behavior of current activities, i.e., normal or attack. In their experiment, they used sleep deprivation attack as a known attack and packet dropping attack as unknown attack. Therefore, their proposed approach is able to detect the both of them. D. Vydeki and R.S. Bhuvaneswaran [12] designed an IDS using Sugeno type-2 FIS to detect the black hole attack. J.Ramkumar and R.Murugeswari [13] proposed a fuzzy logic based IDS to detect and isolate the black hole attack from the network.

3. Problem statement (the black hole attack)

In the black hole attack, a malicious node takes advantage of the route discovery procedure of the reactive routing protocols like AODV [14], to point out itself as having the shortest path to the destination node. This hostile node advertises its convenience of recent routes regardless of checking its routing table in order to gain the route, then it intercepts and deletes all the data that passes through it. Fig. 1 represents the behavior of the black hole attack, in which the source node S wants to establish a route towards the destination node D. In a reactive routing protocol, the source node S broadcasts a RREQ packet to search for a route to the destination node D, all the nodes even the malicious node will receive the RREQ packet, as shown in the Fig. 1 (a). Then, the black hole node will respond directly through a fake RREP packet with a very high destination sequence number to the source node S. Also, the destination node D or a legitimate neighbor node that has the route to the destination node will send a correct RREP packet to the source node S, as shown in Fig. 1 (b). Then, the source node S will choose the largest destination sequence number and the shortest route to send the data packets, according to the design of the reactive routing protocol. Therefore, the source node S would choose the route through the black hole attack. Once the Black hole node has gained the route, it deletes all the data packets as shown in Fig. 1 (c).

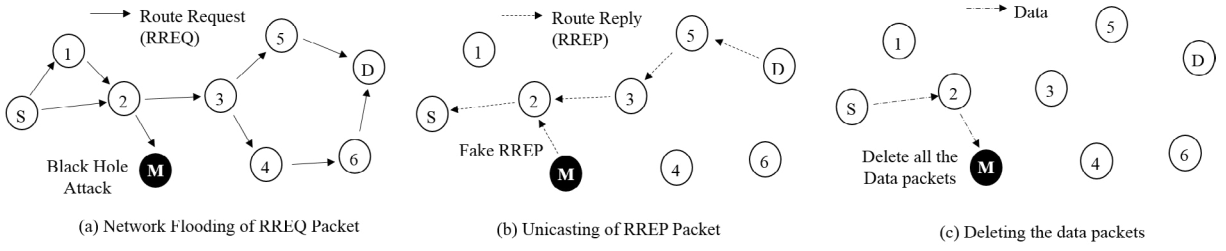

Fig. 1. Black hole attack in AODV.

4. Proposed intrusion detection system

Many studies reported in the literature on the detection of black hole attack are provided by the use of the fuzzy inference system (FIS), which requires human knowledge to select the number of membership functions for each fuzzy set, the position and the shape. Fuzzy rules are also developed based on their experiences. Therefore, it is difficult to optimize these parameters even with a high expert researcher. Consequently, an optimized system is highly recommended to automatically generate fuzzy rules and membership functions. In this paper, an intrusion detection system benefiting from the combination of ANFIS and PSO is proposed to detect the black hole attack. In this proposed IDS, the PSO is applied to improve the performance of ANFIS by adjusting the membership functions and then minimizing the error. The ANFIS predictions make it possible to reconstitute the future behavior of the attacker and thus to detect it.

4.1. Adaptive neuro fuzzy inference system

Adaptive Neuro Fuzzy Inference System (ANFIS) [5] is a technique that incorporates the concepts of fuzzy logic into neural networks. This model simulates the relationship between the input and output of a process through hybrid learning to determine the optimal distribution of membership functions. It is based on the fuzzy " if ... then " rules of Takagi and Sugeno. The architecture of the model has five layers, each with several nodes (see Fig. 2). The square nodes (adaptive) contain parameters, while the circular nodes (fixed) have no parameters in the system. For two input variables x_1 and x_2 given as an example with the only output variable Y, each input variable is described by two linguistic terms: M_1 and M_2 for the variable x_1, L_1 and L_2 for the variable x_2, respectively, hence a rule base "if ... then" described by two fuzzy rules R1 and R2:

$$\begin{aligned} &R1: \text{ if } x_1 \text{ is } M_1 \text{ and } x_2 \text{ is } L_1 \text{ then } y = f_1(x) \\ &R2: \text{ if } x_1 \text{ is } M_2 \text{ and } x_2 \text{ is } L_2 \text{ then } y = f_2(x) \\ &f_1(x) = p_1 x_1 + q_1 x_2 + r_1 \\ &f_2(x) = p_2 x_1 + q_2 x_2 + r_2 \end{aligned} \tag{1}$$

Where p_i, q_i and r_i correspond to the parameters of the conclusion part to be adjusted during the training.

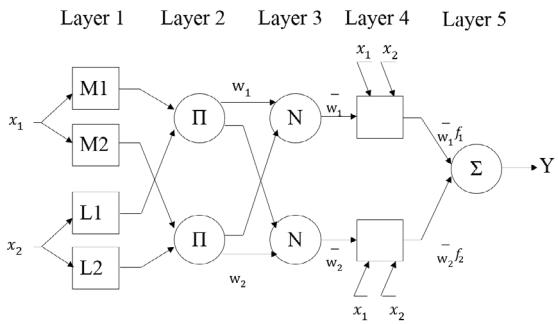

Fig. 2. Architecture of ANFIS algorithm.

4.2. Particle swarm optimization

Particle Swarm Optimization (PSO) [6] is an evolutionary technique that uses a population of candidate solutions to develop an optimal solution to the problem. The degree of optimality is measured by a fitness function. It is inspired by collective behavior and emerging intelligence that exist in societies with organized populations. In its application to optimization problems, this method is based on a set of individuals, initially randomly distributed, called particles and moving in the search space. Each particle is considered as a solution to the problem and has a position X_i and a velocity V_i. In addition, each particle has a memory of its best-visited position P_i and also that of its neighborhood P_g.

4.3. Hybrid approach

The input parameters are chosen in a manner that reflects the existence of a black hole attack. These parameters are Forward Packet Ratio (FPR) and the Average Destination Sequence Number (ADSN).

Forward Packet Ratio (FPR): this parameter can be calculated by dividing the number of the data packets that the neighbor sends by the number of the data packets forwarded to the neighbor.

Average Destination Sequence Number (ADSN): in this parameter we calculate the average of the difference of the destination sequence number in each time interval between the previous sequence number in the neighbor list and the RREP packet.

The proposed ANFIS-PSO algorithm to detect the black hole attack is shown in Fig. 3.

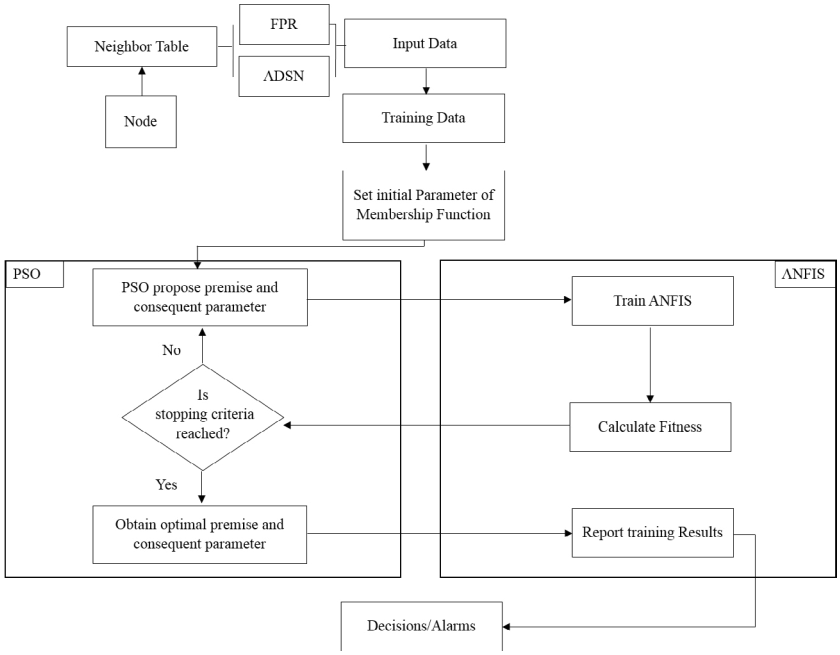

Fig. 3. Flowchart of our proposed IDS.

In this study, a database is extracted from the network, by creating a neighbor table, which records all the activities of the neighbors. Then, FPR and ADSN input parameters are calculated from the database. After that a mapping process is done, where the normal activities with a high fidelity level (10) and abnormal activities with a low fidelity level (0). These input/output dataset is used to train the ANFIS. Then, an NxM matrix that included the premise (membership functions parameters) and consequent parameters is created. Next, these parameters are optimized using the PSO algoritm. The fitness function is defined as the Mean Square Error (MSE) between the measured and experimental data as shown below:

$$MSE = \frac{1}{n}\sum_{i}(A_i - C_i)^2 \tag{2}$$

where A_i and C_i respectively represent the actual and predicted values and n is the number of dataset. The values of premise and consequent parameters in ANFIS model are initially defined randomly and then updated using the PSO algorithm. In other words, PSO will determine the optimal premise and consequent parameters. Then, these optimal parameters are used by ANFIS to extract the final output that corresponds to the prediction of our approach.

5. Experiments

In this section, first we describe the used simulation parameters and performance metrics in the simulation environment. Then, in order to examine the performance of our proposed algorithm, we conducted an experiment under varying the number of connections.

5.1. Simulation Environment

5.1.1. Simulation Parameters

This study used the Network Simulator NS-2 (v-2.35) [15] to simulate the mobile network MANET with/without the black hole attack and MATLAB [16], which is used in the ANFIS + PSO stage in our proposed algorithm. The Table 1 depicted the details of simulation parameters. In this simulation, the network scenario is created by 50 mobile nodes randomly distributed and AODV routing protocol is used. One to twenty pairs were randomly chosen for data communication, each sending 512 bytes per second. For the mobility model of mobile nodes, Random Way Point is used to move the nodes with 0 to 10 m/s and Constant Bit Rate (CBR) is used as traffic type. In the malicious scenario, the black hole node is also randomly distributed. After extraction of data by NS-2, the data is analyzed by MATLAB software.

Table 1. Simulation parameters

Parameter	Value
Coverage Area	800x800m
Number of nodes	50
Simulation time	200s
Transmission range	50m
Mobility model	Random way point
Data Rate	0.25
Packet Size	512 Bytes
Routing Protocol	AODV
Mobility speed	0-10 m/s
No of black hole nodes	1
Connections	2 to 10
Traffic type	UDP–CBR
Pause time	5s

5.1.2. Performance evaluation

Two performance metrics used to evaluate the performance of our proposed system, which are the Detection Rate (DR) and False Alarm Rate (FAR). They can be defined as follows:

$$DR = TP/(TP + FN) \times 100 \tag{3}$$

$$FAR = FP/(TN + FP) \times 100 \tag{4}$$

With:
TP= attack connection record classified as attack (TP).
FP= attack connection record classified as normal (FP).
TN= normal connection record classified as normal (TN).
FN= normal connection record classified as attack (FN).

5.2. Experimental results

The Table 2 shows the detection rate and the false alarm rate of our IDS based ANFIS-PSO algorithm. Based on the table, when the number of connections increases the detection rate gradually decreases and the false alarm rate

increases. This is due to the high false positive rate, which is affected by the changing in the network topology, the traffic and the mobility patterns.

Table 2. Detection Rate and False Alarm Rate.

Metric / Number of connections	1	5	10	15	20
Detection Rate	99.83%	99.83%	99.34%	98.30%	98.35%
False Alarm Rate	0.76%	0.99%	1.33%	1.77%	2.10%

5.3. Conclusion

In this paper, an approach based on ANFIS algorithm combined with PSO for optimization is proposed and applied to detect and prevent the black hole attack. The input parameters of this approach are calculated from an extracted database from the mobile ad hoc network, by creating a neighbor table, which records all the activities of the neighbors. According to the experimental results, our approach has a good detection rate and a low false alarm rate. As a future work, we are planning to compare our IDS with other proposed IDSs to detect black hole attack, also we plan to extend our research to detect more attacks occurred in the mobile ad hoc network.

References

[1] J. Macker, Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations (1999).
[2] H. Moudni, M. Er-rouidi, H. Mouncif, B. El Hadadi, Performance analysis of aodv routing protocol in manet under the influence of routing attacks, in: 2016 International Conference on Electrical and Information Technologies (ICEIT), IEEE, 2016, pp. 536–542 (2016).
[3] H. Moudni, M. Er-Rouidi, H. Mouncif, B. El Hadadi, Attacks against aodv routing protocol in mobile ad-hoc networks, in: 2016 13th international conference on computer graphics, imaging and visualization (cgiv), IEEE, 2016, pp. 385–389 (2016).
[4] T. Anantvalee, J. Wu, A survey on intrusion detection in mobile ad hoc networks, in: Wireless Network Security, Springer, 2007, pp. 159–180 (2007).
[5] J.-S. Jang, Anfis: adaptive-network-based fuzzy inference system, IEEE transactions on systems, man, and cybernetics 23 (3) (1993) 665–685 (1993).
[6] J. Kennedy, Particle swarm optimization, Encyclopedia of machine learning (2010) 760–766 (2010).
[7] H. Moudni, M. Er-rouidi, H. Mouncif, B. El Hadadi, Secure routing protocols for mobile ad hoc networks, in: 2016 International Conference on Information Technology for Organizations Development (IT4OD), IEEE, 2016, pp. 1–7 (2016).
[8] H. Moudni, M. Er-rouidi, H. Faouzi, H. Mouncif, B. El Hadadi, Enhancing security in optimized link state routing protocol for mobile ad hoc networks, in: International Symposium on Ubiquitous Networking, Springer, 2017, pp. 107–116 (2017).
[9] H. Moudni, M. Er-rouidi, H. Mouncif, B. El Hadadi, Modified aodv routing protocol to improve security and performance against black hole attack, in: 2016 International Conference on Information Technology for Organizations Development (IT4OD), IEEE, 2016, pp. 1–7 (2016).
[10] E. V. Balan, M. Priyan, C. Gokulnath, G. U. Devi, Fuzzy based intrusion detection systems in manet, Procedia Computer Science 50 (2015) 109–114 (2015).
[11] A. Chaudhary, V. Tiwari, A. Kumar, Design an anomaly-based intrusion detection system using soft computing for mobile ad hoc networks, International Journal of Soft Computing and Networking 1 (1) (2016) 17–34 (2016).
[12] D. Vydeki, R. S. Bhuvaneswaran, Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks, Journal of Computer Science 9 (4) (2013) 521–525 (2013).
[13] J. Ramkumar, R. Murugeswari, Fuzzy logic approach for detecting black hole attack in hybrid wireless mesh network, in: 2014 IEEE International Conf. on Innovations in Engineering and Technology (ICIET'14), Vol. 2347, 2014, pp. 877–882 (2014).
[14] C. Perkins, E. Belding-Royer, S. Das, Ad hoc on-demand distance vector (aodv) routing, Tech. rep. (2003).
[15] T. Issariyakul, E. Hossain, Introduction to network simulator 2 (ns2), in: Introduction to Network Simulator NS2, Springer, 2009, pp. 1–18 (2009).
[16] D. M. Etter, D. C. Kuncicky, D. W. Hull, Introduction to MATLAB, Prentice Hall, 2002 (2002).