Fuzzy Logic based Intrusion Detection System against Black Hole Attack in Mobile Ad Hoc Networks

Houda Moudni[1], Mohamed Er-rouidi[1], Hicham Mouncif[2] and Benachir El Hadadi[2]

[1]Faculty of Sciences and Technology, Sultan Moulay Slimane University, Beni Mellal, Morocco
[2] Faculty Polydisciplinary, Sultan Moulay Slimane University, Beni Mellal, Morocco

Abstract**:** A Mobile Ad hoc NETwork (MANET) is a group of mobile nodes that rely on wireless network interfaces, without the use of fixed infrastructure or centralized administration. In this respect, these networks are very susceptible to numerous attacks. One of these attacks is the black hole attack and it is considered as one of the most affected kind on MANET. Consequently, 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 of the current activities. Evaluations using extracted database from a simulated network using the Network Simulator NS2 demonstrate the effectiveness of our approach, in comparison to an optimized IDS based ANFIS-GA.

Keywords**:** Mobile Ad Hoc Networks, Intrusion Detection System, Black Hole Attack, ANFIS, PSO**.**

1. Introduction

Nowadays, Mobile Ad hoc NETworks (MANETs) are very attractive, due to its flexibility during the communication between nodes, and also they do not have any predefined infrastructure or centralized management points. In MANETs, each mobile node acts not only as a host to transmit the data packets across the network but also as a router. Due to this ability, MANETs are more desirable for many applications such as disaster relief management, military applications where a rapidly deployable topology of the network is required in the battlefields, communication between groups of people in virtual conferences or neighborhood networks and likewise in many other promising areas.

Similarly to the wired networks, MANETs are also vulnerable to the security attacks such as spoofing and are also prone to other types of attacks [1] [2] [3] due to communication over wireless links, resource constraints (bandwidth and limited power supply), cooperation between mobile nodes and dynamic topology.

This paper concentrates on a specific attack which is the black hole attack that has a big influence on MANETs operations. This attack can be easily launched on reactive routing protocols like AODV [4] routing protocol. In addition, the black hole attacker attracts all the data packets by falsely claiming a shortest and fresh route to the destination node, without having any active route to the specified destination, and then deletes all the data.

From the security point of view, intrusion prevention techniques such as authentication and encryption are not sufficient solutions for MANETs to eliminate the compromised nodes. For this reason, the existence of an Intrusion Detection System (IDS) becomes an essential component of security for MANETs, so it is known as the second line of defense for any network. IDSs can be classified according to the detection techniques used [5]: misuse or signature based detection, specification-based detection, and anomaly-based detection. In the misuse based detection, a comparison between the signature of the existing attack patterns and the network patterns is performed to verify the existence of that intrusion. In the specification-based detection, the system defines a set of specifications that the protocol must satisfy. An attack is detected if an event does not match the established conditions of a good operation. The anomaly detection takes into account the normal behavior of the networks, flag the unknown activity and depending on the activity it generates an alarm.

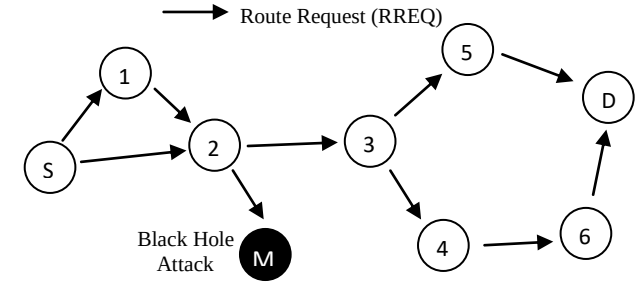
Fuzzy logic [6] is a robust mathematical tool that has been proved its applicability in IDSs. Consequently, many researchers have been proposed fuzzy based IDSs for MANET, but the most of the proposed fuzzy systems make their fuzzy rules based on the human expert knowledge that are lacking of adaptation. For instance, this paper explores the use of a fuzzy system based on adaptation and learning capabilities for intrusion detection system in MANET. For this purpose, the Adaptive Neuro Fuzzy Inference System (ANFIS) [7] is used to automate the process of producing a fuzzy system and then we optimize our system by using the Particle Swarm Optimization (PSO) [8]. This is done by extracting a database from the simulated network, next we extract the appropriate parameters from the database, then a mapping process to these parameters with a target output. Further, we pass the extracted parameters and the target output to the ANFIS to generate the FIS system. And finally, we pass our FIS to the PSO algorithm for optimization.

The subsequent sections are as follows: In Section 2, a brief review of the literature survey. Section 3 presents the black hole attack. Section 4 explains the proposed system. Section 5 illustrates the performance evaluation, including the simulators used, simulation parameters and performance metrics. Section 6 presents the experimental results and discussions. Finally, the last section gives the conclusions and indicates the possible directions for the future work.

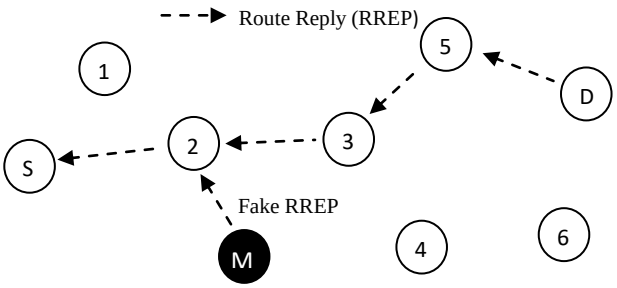
2. Problem Statement and Literature Review

In the black hole attack, a malicious node forges the destination sequence number in the Route REPly Packet (RREP) of the Ad hoc On Demand Distance Vector (AODV)

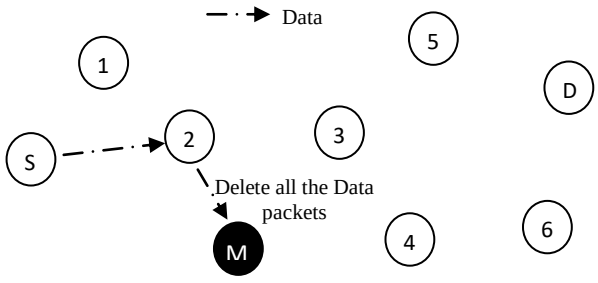
routing protocol [4] in order to drawdown all the packets in the network toward it, then it intercepts and deletes all the data packets passing through it. Fig. 1 represents the behavior of a black hole attack, in which the source node S wants to establish a route to the destination node D. In the AODV routing protocol, the source node S will broadcast a Route REQuest packet (RREQ) to look for a route to the destination node D, in the normal case the legitimate intermediate nodes and also the black hole attack will receive the RREQ packet, as shown in Fig. 1 (a). Then the black hole attack sends a fake RREP immediately without checking its routing table for the route availability, with a very large destination sequence number to the source node S. Likewise, the destination node D or a legitimate neighboring node after checking its routing table sends back a RREP packet to the source node S by reversing the route information stored in the RREQ packet, as shown in Fig. 1 (b). According to the design of AODV, the source node S will choose the largest destination sequence number and the shortest path to send the data packets. Thus, a route through the black hole node would be chosen by the source node S. Once the Black hole node has controlled the route, it can delete all the data packets as shown in Fig. 1 (c).



(a) Network Flooding of RREQ Packet



(b) Unicasting of RREP Packet



(c) Deleting the data packets

Figure 1. Black hole attack in AODV

In a mobile Ad Hoc networks, many techniques exist in the literature to prevent the black hole attack and to provide secure communication among the mobile nodes. They can be a cryptographic origin as in [9] [10] [11] [12], modification in the routing protocol mechanism [13] [14] [15] or the intrusion detection techniques [16].

In this work, we focus on the research done on IDS based fuzzy logic techniques in MANETs. For example, M. Abdel-Azim et al. proposed in [17], an optimization of a fuzzy based intrusion detection system that automate the process of producing a fuzzy system by using an ANFIS for the initialization of the fuzzy inference system and then optimize this initialized system by using the Genetic Algorithm (GA) [18]. In their work, they proved that their optimized proposed IDS against the black hole attack outperforms the normal estimated systems against the same attack. In [19], the authors designed a trust-based routing protocol for clustered-based MANET. The main purpose of their routing scheme is to obtain the most reliable path during the time of the packet transmission from the source node to the destination node. Their mechanism avoids the choice of a malicious node that acts as a real node in ad hoc network. In their paper, they explain how the cluster head calculates its trust score matrix according to the fuzzy logic-based max-min composition of highly reliable nodes. The authors in [20] proposed a new scheme using neuro-fuzzy classifier in binary form for mobile ad hoc networks to identify the behavior of current activities, i.e., normal or abnormal. Their experimental result show that their proposed approach is able to identify known (sleep deprivation attack) and unknown (Packet dropping attack) attacks in ad hoc mobile networks with high positive rate and low false positive rate. In [21], the authors proposed fuzzy based intrusion detection systems in MANET against black hole and gray hole attacks. The proposed system consists of three main blocks which are: attack categorization, fuzzy implementation, and fuzzy estimation. In their fuzzy implementation module, they used the number of packets dropped by the node. The author in [22] proposed a Support Vector Machine (SVM) and fuzzy-based intrusion detection and prevention of MANET attacks. They used SVM to distinguish misbehaving nodes from well-behaved nodes. Then, the fuzzy rules are used to isolate the misbehaved nodes for the prevention of the intrusion. D. Bisen and S. Sharma in [23], also proposed a fuzzy based secure architecture for MANET in which node classification and detection of malicious activity is done through fuzzy detector, by considering the packet delivery ratio (PDR), packet forwarding (PF) and residual energy (RE) as input parameters. After they detect malicious activity, comparative study is performed on the basis of parameters such as a packet delivery ratio, average throughput, total packet forwarding and percentage of detection with variation in node speed. The authors in [24] proposed a Di-Fuzzy logic technique which provide two phase detection for the malicious data packet, and calculates the trustworthiness of the data packet in order to secure the communication between the war troops at different localities. Their technique has three stages, namely, Cluster Head selection, Fuzzy logic technique and Intrusion Detection. The selection of the

cluster head of their solution is based on the node with the maximum energy to improve the lifetime of the network.

3. Proposed Approach

Many works reported in literature related to the detection of black hole attack are provided by the use of Fuzzy Inference System (FIS), which requires the human expert knowledge to choose the number of the membership functions for each fuzzy set, the position, and the shape of each one. The fuzzy rules are also made based on their experiences. Therefore, these parameters are difficult to be optimized even with a high expert researcher. Hence, an optimized system is required in order to automatically generate the fuzzy rules and membership functions. In this paper, an approach benefitting from combination of Adaptive Neuro Fuzzy Inference System (ANFIS) and Particle Swarm Optimization (PSO) is proposed to detect the black hole attack. In this approach, the PSO is applied to improve the performance of ANFIS by adjusting the membership functions and subsequently minimize the error. The ANFIS forecasts permits reconstructing of the future behavior of the attacker and therefore to detect it.

3.1 Input parameters

The input parameters which are extracted from the network must be the most parameters affected by the existence of a black hole attack, in our case would be the Forward Packet Ratio (FPR) and the Average Destination Sequence Number (ADSN). These parameters are extracted from the network by the listening to the traffic promiscuously. Therefore, every node in the network must create a neighbor table for each its direct neighbor node. In this table the following parameter must be stored:

- **Forward Packet Ratio (FPR):** This parameter value calculated on the basis of the number of the packets that the neighbor has been sending on the number of forwarded data packets to a neighbor. The first value can be calculated by counting the number of the data packet each time the direct neighbor sends out a data in promiscuous mode. Then, the second value can be calculated by creating a counter and increment it each time the node sends a data packet to that neighbor.

$$\text{FPR} = \frac{\text{No. of packets the neighbor send}}{\text{No. of forwarded data packets to the neighbor}} \quad (1)$$

- **Average Destination Sequence Number (ADSN):** In the route reply packet of AODV, the destination node transmits its updated sequence number. Whenever a node receives a RREP packet, or sends a data packet to a neighbor or even hears a neighboring node sends data packet, it updates the neighbor table entry for that neighbor with the new values.

In the normal case, the FPR value should be close to 1. Since, when a source node sends a data packet, the intermediate node forwards this data packet to the destination node. In the malicious case, the FPR value would be close to 0. Since, when a source node sends a data packet, the malicious node drops these data. ADSN is equal to the average of the destination sequence numbers that the node receives from its neighbor each time it sends a RREP packet. In the normal case, this average number will be low. The opposite, when a black hole attack exists, this average number will be high, as this malicious node wants to draw down all packets to it.

3.2 Particle Swarm Optimization (PSO)

Particle swarm optimization is a heuristic approach for dealing with the optimization of continuous and discontinuous decision making functions, which proposed by Kennedy and Eberhart in 1995 [8]. The PSO algorithm is a population-based search algorithm based on the biological and sociological behavior of animals such as flocks of birds searching for their food.

In PSO method, each potential solution is represented as a particle in a population (called a swarm). The position of particles is changed constantly in a multidimensional search space until reaching to the equilibrium or optimal state or until computation restrictions are exceeded.

Consider an optimization issue with D variables, a swarm of N particles is initialized in a way that each particle is assigned to an arbitrary position in the D-dimensional hyperspace such that the position of each particle corresponds to a possible answer for the optimization matter. Let x be the position of a particle (coordinate) and v denotes the flight velocity of the particle over a solution space. Every individual x in the swarm is scored using a scoring function, which gets a fitness value representing how well it solves the problem.

A particle's best previous position is represented by Pbest, and Gbest signifies the best particle among all particles in the swarm. Subsequently, all particles that fly over the D-dimensional solution space should follow the rules updated for new positions, until the global optimal position is found. This following deterministic and stochastic update rules shows how a particle's position and velocity are updated:

$$\mathrm{v_i}(\mathrm{t}) = \omega \mathrm{v_i}(\mathrm{t}-1) + \rho_1\left(\mathrm{x}_{\mathrm{pbest_i}} - \mathrm{x_i}(\mathrm{t})\right) + \rho_2\left(\mathrm{x}_{\mathrm{Gbest}} - \mathrm{x_i}(\mathrm{t})\right) \quad (2)$$

$$x_i(t) = x_i(t-1) + v_i(t) \quad (3)$$

where ω represents an inertia weight, ρ1 and ρ2 are random variables. The random variables are defined as ρ1 = r1C1 and ρ2 = r2C2, with $r_1, r_2 \sim U(0,1)$, and C1 and C2 are positive acceleration constants. Fig. 2 illustrates the search mechanism of the PSO algorithm using the speed and the position update rule in (2) and (3). The C1 and C2 represent the weights of the stochastic acceleration terms that push a particle toward Pbest and Gbest, respectively. Small values of the acceleration constants allow a particle to move away from the target regions. In contrast, large values of this constant cause an abrupt displacement of the particles towards the target regions. In this study, constants C1 and C2 are both set at 2.0, following the typical practice in [25]. An appropriate correction of the inertia ω in (3) provides a balance between global and local explorations, as well as the number of iterations when searching for an optimal solution. An inertia correction function "Inertia Weight Approach (IWA)" is used in this paper. During the IWA, the inertia weight ω is modified according to the following equation:

$$\omega = \omega_{\max} - \frac{\omega_{\max} - \omega_{\min}}{\mathrm{Itr}_{\max}} \mathrm{Itr} \quad (4)$$

In (4), ωmax and ωmin represent the initial and final inertia weights, the maximum number of iterations is represented by Itrmax, and the current number of iteration is represented by Itr.

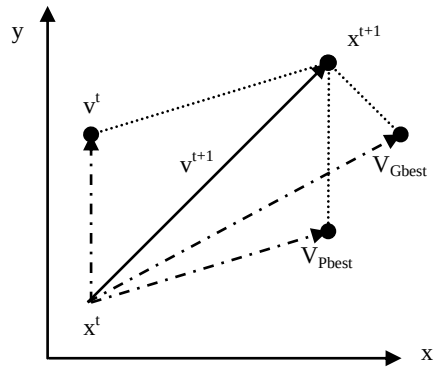


Figure 2. Updating the position mechanism of PSO

3.3 Adaptive Neuro Fuzzy Inference System

The Adaptive Neuro-Fuzzy Inference System (ANFIS) was introduced by Jang [7], referring to the combination of an Artificial Neural Network (ANN) [26] and Fuzzy systems [27] to produce a powerful processing tool. In a neuro-fuzzy system, neural networks automatically extract fuzzy rules from digital data and, through the learning process, membership functions are adaptively adjusted. Also, the parameters related to the membership functions will change depending on the learning process.

Fig. 3 shows the ANFIS architecture. ANFIS can be described as a multi-layered neural network, it is composed of five layers, for which each layer corresponds to the realization of a step of a fuzzy inference system of the Takagi Sugeno type [28].

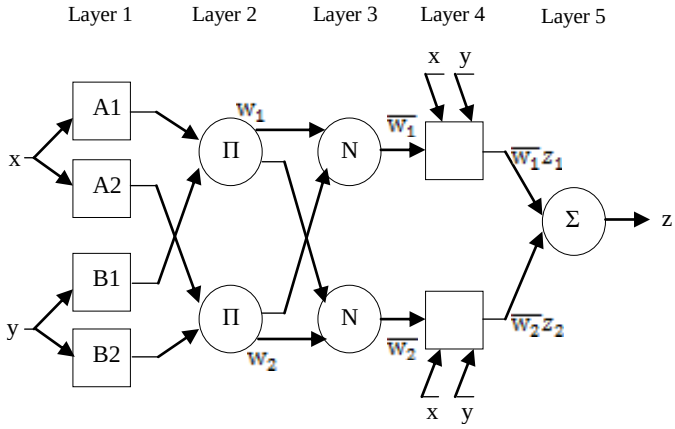


Figure 3. ANFIS architecture

Let O_i^j denotes the output of the ith node in layer j.

Layer 1 contains Membership Functions (MF) of the input variables and feed input values for the next layer. Every node i in the 1st layer is an adaptive node with node function:

$$O_i^1 = \mu A_i(x), \qquad i = 1,2 \qquad (5)$$

Or

$$O_i^1 = \mu B_{i-2}(y), \qquad i = 3,4 \qquad (6)$$

where x (or y) is the input of the ith node and Ai (or Bi-2) is a linguistic label associated with this node. Usually, the membership functions used for A and B are bell-shaped functions with the lowest and highest amounts are 0 and 1, respectively. This membership function is presented in (7):

$$O_i^1 = \frac{1}{1+\left|\frac{x-r_i}{p_i}\right|^{2q_i}} \qquad (7)$$

where {pi, qi, ri} are the parameter set of MFs. As the values of these parameters changes, the bell-shaped function varies accordingly, thus presenting various forms of the membership functions on the linguistic label Ai (or Bi-2).

In the 2nd layer, each node Π multiplies the incoming signals and sends the product as:

$$O_i^2 = w_i = \mu A_i(x)\mu B_i(y), \qquad i = 1,2 \qquad (8)$$

The output of every node indicates the firing strength of a rule.

In the 3th layer, each node N computes the proportion of ith rule of the firing strength to the sum of all rules' firing strengths as:

$$O_i^3 = \overline{w_i} = \frac{w_i}{w_1 + w_2}, \; i = 1,2 \qquad (9)$$

The outputs of this layer are named as normalized firing strengths.

In the 4th layer, each node computes the contribution of the ith rule to the resulting output values from the inference of rules.

$$O_i^4 = \overline{w_i} z_i = \overline{w_i}(a_i x + b_i y + c_i), \qquad i = 1,2 \qquad (10)$$

where wi is the output of the previous layer (layer 3) and {ai, bi, ci} are the parameter set. These parameters are referred to as consequent parameters.

The 5th layer or the output layer contains a single node Σ, which calculates the overall output as the summation of all incoming signals:

$$O_i^5 = \sum_i \overline{w_i} z_i = \frac{\sum_i w_i z_i}{\sum_i w_i} \qquad (11)$$

In this paper, PSO method was used to help ANFIS adjust the parameters of the membership functions. The main advantage of PSO technique is the being less computationally expensive for a given size of network topology. In this study, the membership functions considered are triangular-shaped.

3.4 ANFIS-PSO Algorithm

In this section, our proposed optimized system is described step-by-step and presented in Fig. 4.

First step (1): There are two types of learning updates: online learning and batch learning. The first type of learning updates the network after each example, and the other type waits for the entire learning set, and then updates the network, which is the one chosen for that proposed system. For this to be possible, a database must be extracted from the

network. This is done by creating a neighbor table recorder that records all the activity of the neighbors table in all nodes of the network. Then, a mapping process must be set up, where the normal activities with a high fidelity level (10 in our case) and abnormal activities with a low fidelity level (0 in our case). After the data mapping process, FPR and ADSN input parameters must be calculated from the database as explained earlier, therefore three sets of data are presented the FPR set and the ADSN set as the inputs sets and the target FL as the output set. The whole data are divided into two groups: training dataset (two-third of the entire datasets) and testing dataset (the rest of the datasets).

Second step (2): Train the ANFIS with the training dataset from the implementation of the previous step. The training process allows the system to adjust its parameters as inputs/outputs. The ANFIS is trained till the designated number of times is reached or the results are obtained with minimum error. After defining the learning data, the type of membership functions and the number of times, the system is optimized by adjusting the parameters of membership functions. We use PSO to train the parameters associated with the membership functions of the fuzzy inference system.

Third step (3): Let N be the number of membership functions, therefore we create a vector with N-dimension. This vector contains the parameters of the membership function and will be optimized by the PSO algorithm. The fitness function is defined as the Mean Squared Error (MSE).

Fourth step (4): In this step we define the parameters associated with the PSO algorithm as shown in Table 1.

Table 1. Parameters of the PSO algorithm

Parameters	Value
Number of particles	25
Number of iterations	1000
Cognitive acceleration C1	2.0
Social acceleration C2	2.0
Initial inertia weight ωmin	0.9
Final inertia weight ωmax	0.4

The parameters are initialized randomly in the first step and are then updated using the PSO algorithm. At each iteration, one of the parameters of the membership function is being updated. For example, in the first iteration pi is updated then in the second iteration qi is updated and after updating all the parameters, again the first parameter update is considered and so on. These parameters are grouped together in a vector that is being updated in each iteration. The PSO algorithm is used to optimize the membership function parameters is described below:

a) Initialize the positions and speeds of the population. For each particle, the position and velocity vectors are randomly initialized with the same size as that presented by the size of the problem;

b) Evaluate the ability of the individual particle (Pbest). If the value is better than the current value of the individual particle, Pbest resets the current position of the particle and updates the individual value. If the best of all the particles of individual values is better than the overall value of the current Gbest reset the location of the best particles;

c) Measure the fitness function of each particle (Pbest) and store the particles with the best fitness value (Gbest);

d) Change the speed according to the position Pbest and Gbest;

e) Update the particles;

f) Stop if the condition is verified. If the current number of iterations reaches the maximum number by default or if the result reaches a minimum error threshold, stop the iteration and collect the best solution.

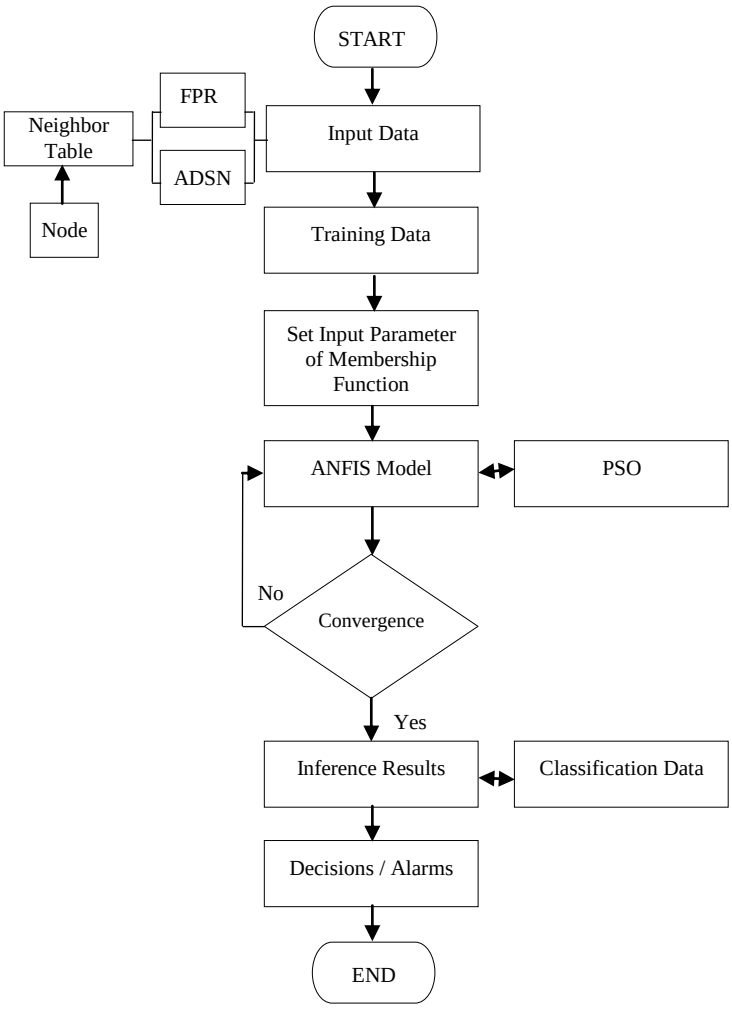


Figure 4. Flowchart of our proposed approach

Fifth step (5): Extract the output from the ANFIS using the parameters found by the PSO algorithm.

Sixth step (6): The final output corresponds to the prediction of our approach.

4. Performance Evaluation

In this section, we describe the used simulators, simulation parameters and performance metrics.

4.1 Simulators

In this work, we used three simulators: Network Simulator NS-2 (v-2.35) [29], which used in the simulation of the mobile network MANET, simulation of the black hole attack and the optimized IDS against the black hole nodes. The second simulator is MATLAB [30], which used in the ANFIS stage, and PSO stage in our proposed algorithm, the last simulator used is the QTFUZZYLITE [31], which used

to encode the fuzzy interface system into a C++ code to be added into our IDS in NS2.

4.2 Simulation Parameters

In these simulations, we consider 50 mobile nodes move within a square field of 800×800 m. One pair to twenty pairs were randomly chosen for data communication, each sending 512 bytes per second. All nodes were moved in a Random-way point model, with random speeds ranging between 0 and 10m/s. In addition, the pause time between movements is 5s with 200s of simulated time. For the malicious node is also randomly distributed. All the simulation parameters are summarized in Table 2. Each data point represents an average of twenty different runs. We execute the network in three situations. Situation 1: we simulate the network without the presence of black hole attack. Situation 2: we simulate the network under the presence of black hole attack and without the presence of IDS. Situation 3: we simulate the network under the black hole attack and the presence of our proposed intrusion detection system.

Table 2. Simulation parameters

Parameter	Value
Coverage Area	800x800 m
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 / AODV-with attack / IDS-AODV
Mobility speed	0-10 m/s
No of black hole nodes	1
Connections	2 to 10
Traffic type	UDP–CBR
Pause time	5s

4.3 Performance Metrics

In order to evaluate the performance of our protocol, we have used the following metrics:

- **Packet Delivery Ratio (PDR):** This is the ratio of the total number of data packets received by the destination nodes to the total number of data packets generated by the source nodes. Therefore, the packet delivery rate shows the total number of data packets that reach the destination successfully. A higher packet delivery rate shows higher protocol performance.
- **Average End-to-End Delay:** It can be defined as the time elapsed between the time of sending of a bit by the source node and the time of its reception by the destination node. It includes all the possible delays taken by the router to look for the path in the network such as buffering during route discovery latency, propagation, queuing at the interface queue, MAC retransmission delays and transfer time. The average end-to-end delay is measured in seconds.
- **Normalized Routing Overhead (NRO):** This metric indicates the number of routing control packets generated per data packets transmitted.

In addition, two performance metrics used to evaluate the performance of the proposed system in case of the presence of black hole attack, the Detection Rate (DR) and False Alarm Rate (FAR). They can be calculated using the confusion matrix in Table 3 and defined as follows:

$$DR = TP/(TP+FN)\times 100 \quad (12)$$

$$FAR = FP/(TN+FP)\times 100 \quad (13)$$

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).

Table 3. Confusion Matrix for Evaluation of Intrusions (Attacks)

Confusion Matrix (Standard Metrics)		**Predicted Connection Label**	
		Normal	***Intrusions (Black Hole Attack)***
Actual Connection label	***Normal***	True Negative (TN)	False Alarm (FP)
	Intrusions (Black Hole Attack)	False Negative (FN)	Correctly detected Attacks (TP)

5. Experimental Results and Discussion

The performance of our proposed IDS is evaluated and compared with the optimized intrusion detection system which use ANFIS and Genetic Algorithm (GA) for optimization proposed in [17]. The simulation was running on a laptop with a processor Core i5 and 4GB RAM with Linux Ubuntu version 12.04 as an operating system. Each run is executed with a random sources and destinations pairs from one to twenty pairs, for each one the network simulated in four different situations (the basic AODV, with black hole attack, with our proposed IDS, and with the optimized IDS proposed in [17]).

Fig. 5 shows the variation of the packet delivery ratio with the modification of the connection number. As the number of connections increases, the packet dropping increases due to congestion; therefore, the PDR chart for the standard AODV begins to decrease as the number of sources increases. It is clear from the figure that the PDR of our proposed IDS is superior over the basic AODV under black hole attack or the optimized IDS. Fig. 6 depicts the average end-to-end delay. All protocols have a higher end-to-end delay with a high number of connections. Mainly because frequent routes break down due to death of intermediate nodes and mobility. Also, we observe that our IDS and the optimized IDS using ANFIS+GA under black hole attack is slightly increased in the average end-to-end delay, compared to the standard AODV. This is due to the additional waiting time in each intermediate node before sending the reply packet. The average end to end delay in the presence of the black hole attack is the least in all the situations, since the malicious node sends the route reply immediately without checking its routing table for the route availability. The normalized

routing overhead is shown in Fig. 7 while varying the number of connections. As we can see the routing overhead of our IDS and the IDS based ANFIS and GA is slightly higher compared to the standard AODV because of the additional process involved to avoid the selection of malicious nodes. Also, the use of the alarm messages in order to inform the other nodes about the black hole attack. The NRO in case of the AODV under black hole attack is lower than the other situations, due to that the malicious node manipulates the network to think that it delivers the data packets when in fact it does not.

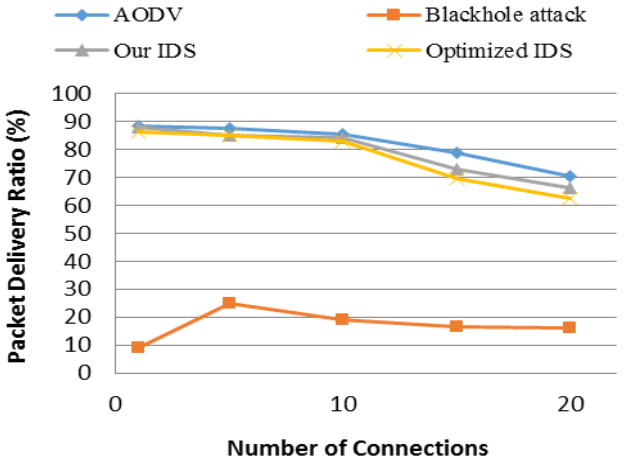


Figure 5. Packet delivery ratio vs. number of connections

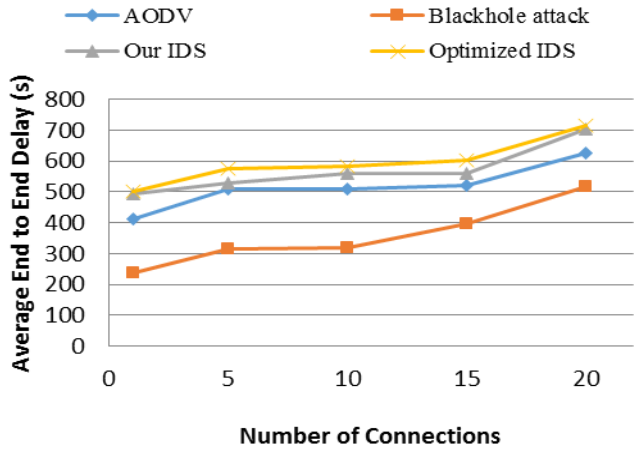


Figure 6. Average end to end delay vs. number of connections

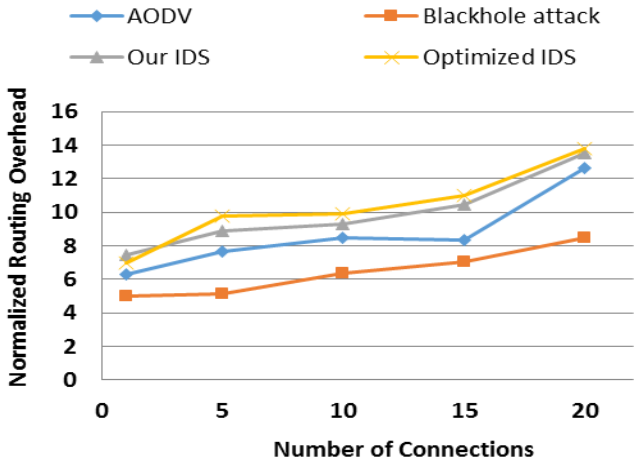


Figure 7. Normalized routing overhead vs. number of connections

In the context of evaluation of the classification measurement of our IDS and the optimized IDS proposed in [17], the detection rate and false alarm rate was performed in Table 4. The test results show that our proposed IDS has the best performance with high detection rate and low false alarm rate when we varying the number of connections. As a result, it is proven to say that the use of our proposed IDS provides a much robust IDS comparing with the optimized IDS which use ANFIS and GA.

Table 4. Detection Rate and False Alarm Rate

Number of connections	Our IDS		The optimized IDS	
	Detection Rate	False Alarm Rate	Detection Rate	False Alarm Rate
1	99.83%	0.76%	99.75%	0.85%
5	99.81%	0.99%	99.82%	1.23%
10	99.34%	1.33%	99.30%	1.29%
15	98.30%	1.77%	98.21%	1.93%
20	98.35%	2.10%	98.11%	2.76%

6. Conclusions

In this paper, we proposed a novel method for detecting and preventing the effect of a black hole attack. In our novel method we initialize the FIS by ANFIS approach, then we optimize the initialized system by using the PSO algorithm. The effectiveness of this approach is evaluated by comparing it with an optimized IDS proposed by another author which use the ANFIS approach combined with GA. According to the experimental results, our approach has a good detection efficiency against the black hole attack, but with a slight increase in normalized routing overhead. As a future work, we are concentrating to extend our research to detect more attacks in a mobile ad hoc network.

References

[1] 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 Electrical and Information Technologies (ICEIT), 2016 International Conference on. IEEE, pp. 536-542, 2016.

[2] H. Moudni, M. Er-rouidi, H. Mouncif, B. El Hadadi, "Attacks against AODV routing protocol in Mobile ad-hoc networks," In Computer Graphics, Imaging and Visualization (CGiV), 2016 13th International Conference on. IEEE, pp. 385-389, 2016.

[3] B. Wu, J. Chen, J. Wu, M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," In Wireless network security, Springer, Boston, MA, pp. 103-135, 2007.

[4] C. Perkins, E. Belding-Royer, S. Das, "Ad hoc on-demand distance vector (AODV) routing," No. RFC 3561, 2003.

[5] A. Nadeem, M. P. Howarth, "A survey of MANET intrusion detection & prevention approaches for network layer attacks," IEEE communications surveys & tutorials, Vol. 15, No 4, pp. 2027-2045., 2013.

[6] J. Yen, R. Langari, "Fuzzy logic: intelligence, control, and information," Upper Saddle River, NJ: Prentice Hall, Vol. 1, 1999.

[7] J. S. Jang, "ANFIS: adaptive-network-based fuzzy inference system," IEEE transactions on systems, man, and cybernetics, Vol. 23, No 3, pp. 665-685, 1993.
[8] J. Kennedy, "Particle swarm optimization," In Encyclopedia of machine learning, Springer US, pp. 760-766, 2011.
[9] H. Moudni, M. Er-rouidi, H. Mouncif, B. El Hadadi, "Secure routing protocols for mobile ad hoc networks," In Information Technology for Organizations Development (IT4OD), 2016 International Conference on IEEE, pp. 1-7, 2016.
[10] R. Al-Mutiri, M. Al-Rodhaan, Y. Tian, "Improving Vehicular Authentication in VANET Using Cryptography," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 10, No 1, 2018.
[11] 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, Cham, pp. 107-116, 2017.
[12] A. Sharma, D. Bhuriya, U. Singh, "Secure data transmission on MANET by hybrid cryptography technique," In Computer, Communication and Control (IC4), 2015 International Conference on. IEEE, pp. 1-6, 2015.
[13] H. Moudni, M. Er-rouidi, H. Mouncif, B. El Hadadi, "Modified AODV routing protocol to improve security and performance against black hole attack," In Information Technology for Organizations Development (IT4OD), 2016 International Conference on. IEEE, pp. 1-7, 2016.
[14] S. Shahabi, M. Ghazvini, M. Bakhtiarian, "A modified algorithm to improve security and performance of AODV protocol against black hole attack," Wireless Networks, Vol. 22, No. 5, pp. 1505-1511, 2016.
[15] J. Swain, B. K. Pattanayak, B. Pati, "A New Approach for DDoS attacks to discriminate the attack level and provide security for DDoS nodes in MANET," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 9, No. 3, pp. 450-456, 2017.
[16] M. Zeeshan, H. Javed, S. Ullah, "Discrete R-Contiguous bit Matching mechanism appropriateness for anomaly detection in Wireless Sensor Networks," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 9, No. 2, pp. 157, 2017.
[17] M. Abdel-Azim, H. E. D. Salah, M. Ibrahim, "Black Hole attack Detection using fuzzy based IDS," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 9, No. 2, pp. 187, 2017.
[18] D. E. Goldberg, J. H. Holland, "Genetic algorithms and machine learning," Machine learning, Vol. 3, No. 2, pp. 95-99, 1988.
[19] J. Kundu, K. Majumder, D. De, "An Efficient Trust-Based Routing Scheme by Max-Min Composition of Fuzzy Logic for MANET," In Proceedings of the International Conference on Recent Cognizance in Wireless Communication & Image Processing, Springer, New Delhi, pp. 435-440, 2016.
[20] A. Chaudhary, V. N. 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, Vol. 1, No. 1, pp. 17-34, 2016.
[21] E. V. Balan, M. K. Priyan, C. Gokulnath, G. U. Devi, "Fuzzy based intrusion detection systems in MANET," Procedia Computer Science, Vol. 50, pp. 109-114, 2015.
[22] A. A. Lakshmi, K. R. Valluvan, "Support vector machine and fuzzy-based intrusion detection and prevention for attacks in MANETs," International Journal of Mobile Network Design and Innovation, Vol. 6, No. 2, pp. 63-72, 2015.
[23] D. Bisen, S. Sharma, "Fuzzy Based Detection of Malicious Activity for Security Assessment of MANET," National Academy Science Letters, Vol. 41, No. 1, pp. 23-28, 2018.
[24] W. G. Theresa, S. Sakthivel, "Fuzzy based intrusion detection for cluster based battlefield MANET," In Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2017 IEEE International Conference on. IEEE, pp. 22-27, 2017.
[25] J. Kennedy, "The behavior of particles," In International Conference on Evolutionary Programming, Springer, Berlin, Heidelberg, pp. 579-589, 1998.
[26] S. C. Wang, "Artificial neural network," In Interdisciplinary computing in java programming, Springer, Boston, MA, pp. 81-100, 2003.
[27] R. Kruse, J. E. Gebhardt, F. Klowon, "Foundations of fuzzy systems," John Wiley & Sons, Inc, 1994.
[28] J. M. Mendel, R. I. John, F. Liu, "Interval type-2 fuzzy logic systems made simple," IEEE transactions on fuzzy systems, Vol. 14, No. 6, pp. 808-821, 2006.
[29] T. Issariyakul, E. Hossain, "Introduction to network simulator NS2," Springer Science & Business Media, 2011.
[30] D. M. Etter, D. C. Kuncicky, D. W. Hull, "Introduction to MATLAB," Prentice Hall, 2002.
[31] J. F. Rada-Vilela, "A fuzzy logic control library in C++," In Proceedings of the Open Source Developers Conference, 2013.