Black Hole attack Detection using Fuzzy based IDS

Mohammed Abdel-Azim[1], Hossam El-Din Salah[2], Menas Ibrahim[3]

[1, 2, 3] Engineering Department - Faculty of Engineering - Mansoura University, Egypt

***Abstract*:** In the past few years, an evolution in the wireless communication has been emerged, along with the evolution a new type of large potential application of wireless network appears, which is the Mobile Ad-Hoc Network (MANET). Black hole attack considers one of the most affected kind on MANET. Therefore, the use of intrusion detection system (IDS) has a major importance in the MANET protection. In this paper, an optimization of a fuzzy based intrusion detection system is proposed which automate the process of producing a fuzzy system by using an Adaptive Neuro-Fuzzy Inference System (ANFIS) for the initialization of the FIS and then optimize this initialized system by using Genetic Algorithm (GA). In addition, a normal estimated fuzzy based IDS is introduced to see the effect of the optimization on the system. From this study, it is proven that the optimized proposed IDS perform better that the normal estimated systems.

***Keywords*:** Black Hole attack, ANFIS, GA, FIS.

1. Introduction

Due to the flexibility of the MANET, its application grows rapidly in the past few years. This type of network allows a large number of wireless nodes to communicate with each other with ease, as there is no fixed infrastructure to be installed first [1-3]. Therefore, this kind of network is very effective for military application. Each node in the network requests a communication with other nodes by the use of various type of routing protocol [4] such as Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), also it relays on the routing protocol to transfer data from one node to another.

The MANET, which is a wireless network, it does not inherit the vulnerabilities of a regular wireless network only but also it has its own vulnerabilities such as [5]: lack of centralized node, no predefined Boundary, limited power supply, bandwidth constraint, security, and dynamic topology. Being used first on the military battlefield, the security vulnerability is one of its main vulnerability. Intrusion prevention techniques like encryption, authentication, and firewall are not sufficient to secure the network from MANET attacks, also MANET routing protocols run under an assumption that all the nodes in the network works cooperatively with each other and not maliciously. For this reason, the existence of an intrusion detection system in MANETs becomes very important [6]. Intrusion detection system can be classified into three types [7]: signature based detection, specification-based detection, and anomaly-based detection. In the signature base detection, a comparison between the signature of existing attack patterns and the network pattern is done to check the existence of that attack. The anomaly detection classified into knowledge, statistical, and learning based. The anomaly detection considers the normal behavior of networks, flag the unknown activity and based on the activity it generates an alarm [8].

Black hole, which is a DoS attack MANET attack [9, 10], is a type of attack that has a big influence on the network. It attacks the network layer, which is responsible for route advertising by attacking the network layer protocols like AODV routing protocol.

Fuzzy logic is a mathematical tool that provides a computational paradigm to deal with the imprecision and the uncertainty involved in human reasoning known as approximate reasoning. The characteristic of FL, which is, it is capable of expressing knowledge in a linguistic way, makes the systems based on fuzzy logic suitable for applications such as IDS. Many researchers proposed fuzzy-based IDS to detect the black hole attack but as explained later fuzzy based IDS has some difficulty in specifying the parameters of the membership function, which relay on the user's experience, his understanding of the network or even on trial and error. In this paper, a proposed IDS is introduced to automate the process of producing a fuzzy system by using ANFIS and then optimizes this system using the GA. This done by extracting a database from the simulated network, extracts suitable parameters from that database, maps these parameters with a target output, then passes the extracted parameters and the target output to an ANFIS to generate FIS, and then passes the FIS to a GA system for optimization. In addition, a comparison between normal estimated fuzzy interface system and the optimized fuzzy interface system is done to evaluate the performance of the two systems.

The rest of this paper is organized as follow: (i) Section-2: is a brief literature survey; (ii) Section-3: is the problem statement; (iii) Section-4: proposed systems; (iv) Section-5: illustrates the performance evaluation including the simulator used, simulation methodology and performance metrics; (v) Section-6: provides the results are discussions, and (vi) Section-7: introduces the conclusions and future works.

2. Literature Survey

Wahengbam, and Marchang in [11] proposed fuzzy-based IDS which prevent three types of attacks which are packet forwarding misbehavior, black hole attack, and gray-hole attack. The parameters used in work were the number of packets lost and the number of packets forwarded by the node. Balan, and et al. in [12], also proposed fuzzy-based IDS for black hole and gray-hole attack, the proposed system consists of three main blocks they are: attack categorization, fuzzy implementation, and fuzzy estimation. The number of packets dropped by the node is used in the fuzzy implementation module. Sujatha, and Dharmar [13] proposed IDS, which depend on genetic algorithm. The used parameters are the number of packets drop, request-forwarding rate, and route request rate. Kurosawa, and et al. [14] proposed an active routing protocol known as secure AODV routing for analysis of the effect of the black hole attack when the destination sequence number are changed via simulation. Then, we select features in order to define the provides state from the characteristic of black hole attack. Yunwu [15] proposed a fuzzy based genetic algorithm,

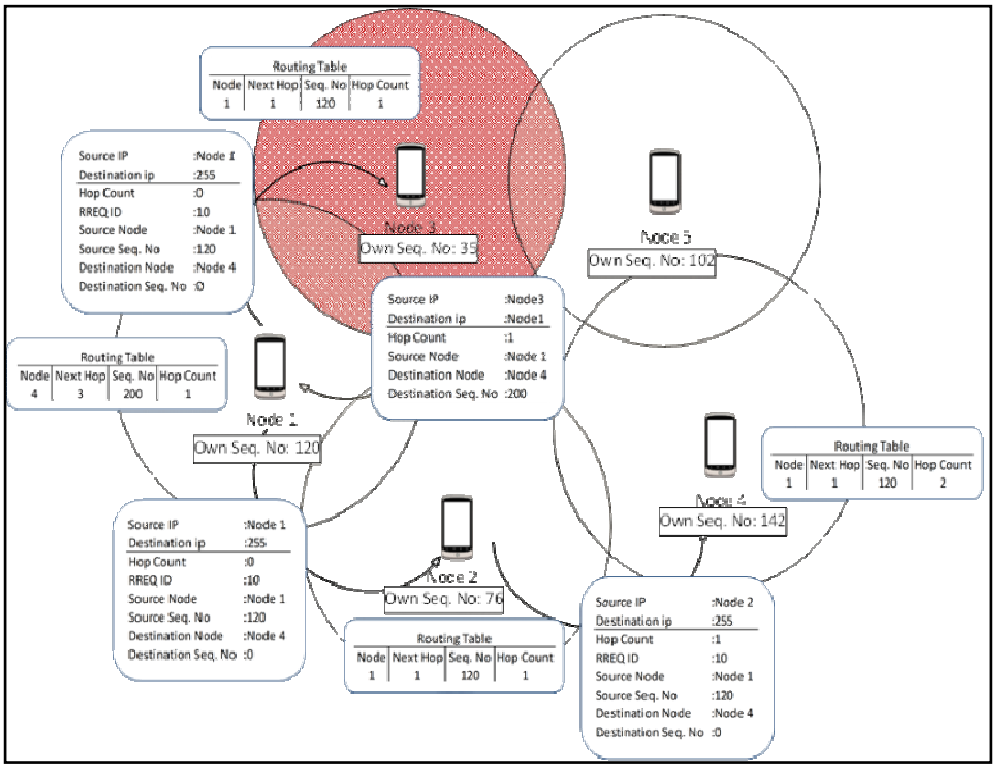

Figure 1. The black hole attack process

which gets initial rules from fuzzy and uses the genetic algorithm for the final rules. Anuar et al. [16] proposed IDS based o multi-agent with CI techniques. In addition, they analyzed the limitations, significance of different prevention mechanisms and IDS. Pimprale and Joshi [17] proposed a technique using multi-boosting and binary classifier for the reduction of bias and variance. The use of binary classifier in feature selection evaluated the performance in the presence of the arrival of new attack. Abinaya and Govindarajan [18] proposed simultaneous classification and detection to assure more efficient security approaches in comparison with traditional approaches. Morgera et al. [19] provides a survey of IDS for MANET, IDS techniques in general, and IDS for the application layer in the WSN. Sharma et al. [20] proposed multilevel IDS by the use of multi-agent. This is done by storing different type of attack in a database and then analyze the dependency of arrival type with the database; the subject behavior analysis is used in IDS.

3. Problem Statement

3.1. Black Hole Attack

Due to the nature and the properties of the MANETs, that prompt it for many applications such as in battlefield and business conferences [21], there is a need for securing the data transferred between any communication nodes. Therefore, recently many researchers introduce secure routing protocols. This secure routing protocols designed to secure the data by providing (i) non- reputation technique and identity authentication; (ii) integrity; (iii) availability of resources; and (iv) privacy and confidentiality. Black hole attack [22] consider a Denial of Service (DoS) attack, routing attack in MANET [23]. It works by drawdown the packets in the network to it and then drops, alters the content of the packets, or even passes the packets to another malicious node. This is done by sending a fake RREP to any source node claiming that it has a route to the desired destination even if no such route exists. For more explanation assume the situation in Figure 1, when node 3 receives the RREQ message from node 1 it immediately sends back a fake RREP message to node 1 with a fake destination sequence number. Noticing that node 1 will receive two RREP messages. The first one from node 2 that has a destination sequence number with 143 as a value, which is the correct route to the destination. The second RREP message is from node 3, which has a destination sequence number of with 200 as a value, which is the fake route to the destination. However, the source node will choose the path through node 3 because it thinks that it has the fresh route. Thinking that it makes the correct choice node 1 will send the packet to node 3 assuming that it will pass it to node 4 when it fact it will drop the packets.

4. Proposed Systems

In many types of research, the solution of detection the black hole attack comes with the use of FIS, which relies on the researcher experience to understand the system very well in order to choose the number of the membership functions for each fuzzy set, the shape, and the position of each one. In addition, it requires an effort from the researcher's hand to set the rule base for that fuzzy system (noticing that even with a high expert researcher these parameters are difficult to be optimized). In order to see the effectiveness of the optimization process in discovering the black-hole attack two systems was introduced. The first system is the normal estimated one, which relays only on our understanding of the system to choose the parameter of the fuzzy system, which would be referred to "normal system". The other proposed system, which would be referred to "optimized system", will automate and optimize the parameters of FL and minimize

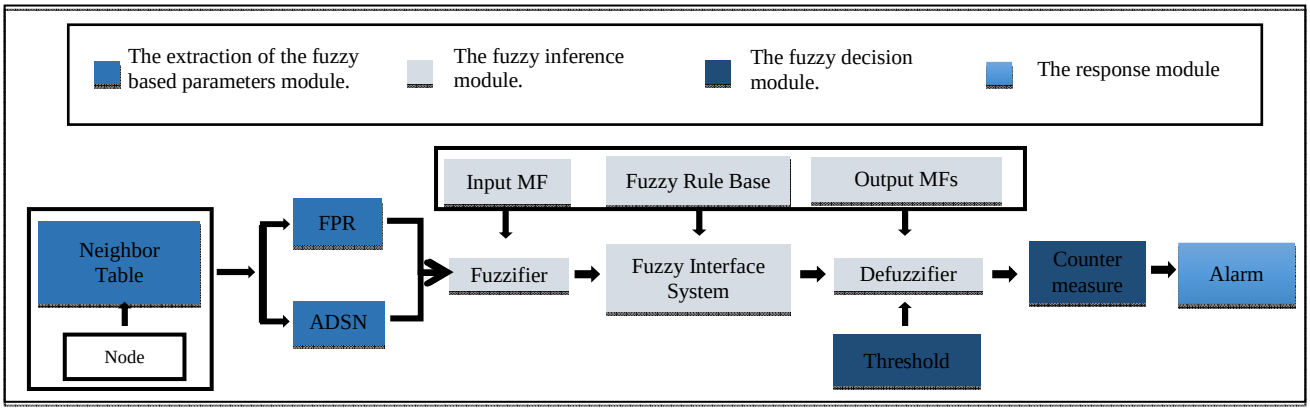

Figure 2. The normal proposed system in detail

the error by using ANFS and GA systems. A similar optimization process used for grade estimation in [24].

4.1. Normal System

The normal fuzzy logic based intrusion detection system consists of four main modules, which are: (i) Extraction of the fuzzy based parameters module; (ii) Fuzzy inference module; (iii) Fuzzy decision module; and (iv) Response module. In the extraction of fuzzy based parameters process, the system extracts the desired parameters for analysis from network traffic and then passed these parameters to the fuzzy interface module. In fuzzy interference module, fuzzy rules and membership functions are performed on these parameters to find the fidelity level of each node in the network after that the fidelity the of each node is compared to a threshold value for finding out the behavior of each node in fuzzy decision module. If the calculated fidelity level is less than the chosen threshold value, the node will be considered malicious and the response module will be activated. Figure 2 illustrates how the four modules interact

4.1.1. Extraction of Fuzzy Based Parameters

The input parameters to the fuzzy interface must be the parameters that affected most by the existence of black hole attack, which in this case would be the forward packet ratio (FPR) and the average destination sequence number (ADSN). Each node in the network must create a neighbor table in it so it can extract those parameters from the network. In the neighbor table, the node stores each direct neighbor, which can communicate directly with it. For each direct neighbor the following parameter must be stored:

- The number of forwarded data packets to a neighbor which can be calculated by creating a counter and increase it by one each time the node sends a data packet to that neighbor.
- The no. of the packets that the neighbor has been sending which can be calculated be making the node listen to the network traffic promiscuously and then creating another counter which increased by one each time the neighbor send out a data packet.
- The destination sequence numbers that the node receives from the neighbor each time it sends an RREP message to it. Every time a node receive an RREP message or send a data packet to a neighbor or even hear a neighbor send data packet it updates the neighbor table entry for that neighbor with the new values.

FPR and ADSN for each neighbor can be computed from the neighbor table as follows:

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

For a normal intermediate node when a source node send a data packet to it the intermediate node forward that data packet toward the destination so in normal cases the value or FPR must be close to 1. In the case of attack node when a source node sends a data packet to it the attack node drops the packet so, in this case, the value of the FPR would be close to 0. ADSN is equaled to the average of the destination sequence numbers that the node receives from the neighbor each time it sends a REEP message to it.
For a normal intermediate node this number will be low but in case if attack this number will be high, as it wants drawdown all packet to it.

Table 1. The Rule base of Mamdani FIS

S.NO.	FPR	ADSN	FL
1	Low	Low	Low
2	Low	Medium	Low
3	Low	High	Low
4	Medium	Low	Medium
5	Medium	Medium	Medium
6	Medium	High	Low
7	High	Low	High
8	High	Medium	High
9	High	High	Low

4.1.2. Fuzzy Inference Module

In the normally proposed system, a Mamdani fuzzy inference system is used to evaluate the behavior of a node in the network. This system receives two input parameters from the neighbor table which are Forward Packet Ratio and Average Destination Sequence Number and offer only one output parameter, Fidelity Level to check if a node malicious or normal. The rule bases [25] are presented in Table 1 for evaluating the behavior of the node. Membership functions are selected for inputs and the output parameters as in Figure 3. The first rule in the rule base in fuzzy inference system is

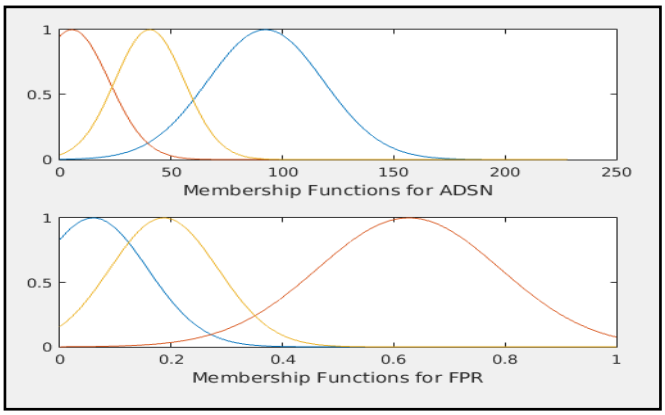

Figure.3 The membership function for the normal proposed system

explained as follows: If Forward Packet Ratio is Low and Average Destination Sequence Number is Low then Fidelity Level is high. Fidelity Level (which lay between 0 and 10) of each neighbor in the neighbor in each node is calculated every T sec (5 sec in the proposed system).The low value of Fidelity Level shows a more malicious behavior of a node than a normal behavior. Therefore, Fidelity Level of value 0 indicates the neighbor node is completely malicious and 10 indicate a completely normal behavior.

4.1.3. Fuzzy Decision Module

In this module, a threshold value is used to determine if a node is malicious or not as if the calculated value of fidelity level of this is less than the threshold value this node considered malicious. In the proposed system, a value of 3 is set as the threshold value.

4.1.4. Response Module

- If the node checks to be malicious, four actions are done:
- Delete the route to the malicious node from the routing table.
- Adding this malicious node to a created blacklist.
- Prevent the node from processing any route reply message comes from any node in that black list.
- Sending AODV message, which would be IDS message to inform other nodes about the malicious node.

4.2. Optimized System

The proposed optimized system consider the automated version of the normal system as mentioned the choice of the number, shape, and position of the membership functions along with the determination of the rule base can be hard and not always optimal. Therefore, the optimized system differed from the normal system only in the fuzzy interface module with the same Extraction of fuzzy based parameters module, Fuzzy decision module, and response module. To optimize the fuzzy interface module an optimization process is done which includes three stages: Data preparations stage, ANFS stage, and GA stage. Figure 4 shows the effect of the optimization process on the system.

4.2.1 Data Preparations Stage

There are two types of learning updates: on-line learning, which updates the network after each exemplar, and batch learning, which waits for the entire training set and then updates the network. Batch learning is the one chosen for this proposed system. To make this possible a database must be extracted first from the network. This is done by creating a neighbor table recorder which record all the neighbor table activity in all the nodes in the network including the source nodes the destination nodes and also the intermediate nodes, after that a mapping process must be done which mapped the normal behavior entries with a high Fidelity level target (10 in our case), and the abnormal behavior entries with a low Fidelity level target (0 in our case), the abnormal entries is known by the IP address of the malicious nodes (in learning process the IP address of the malicious node must be known only to know the characteristics of the FPR, ASDN parameters in the presence of attack but after learning process it can be any node in the network).

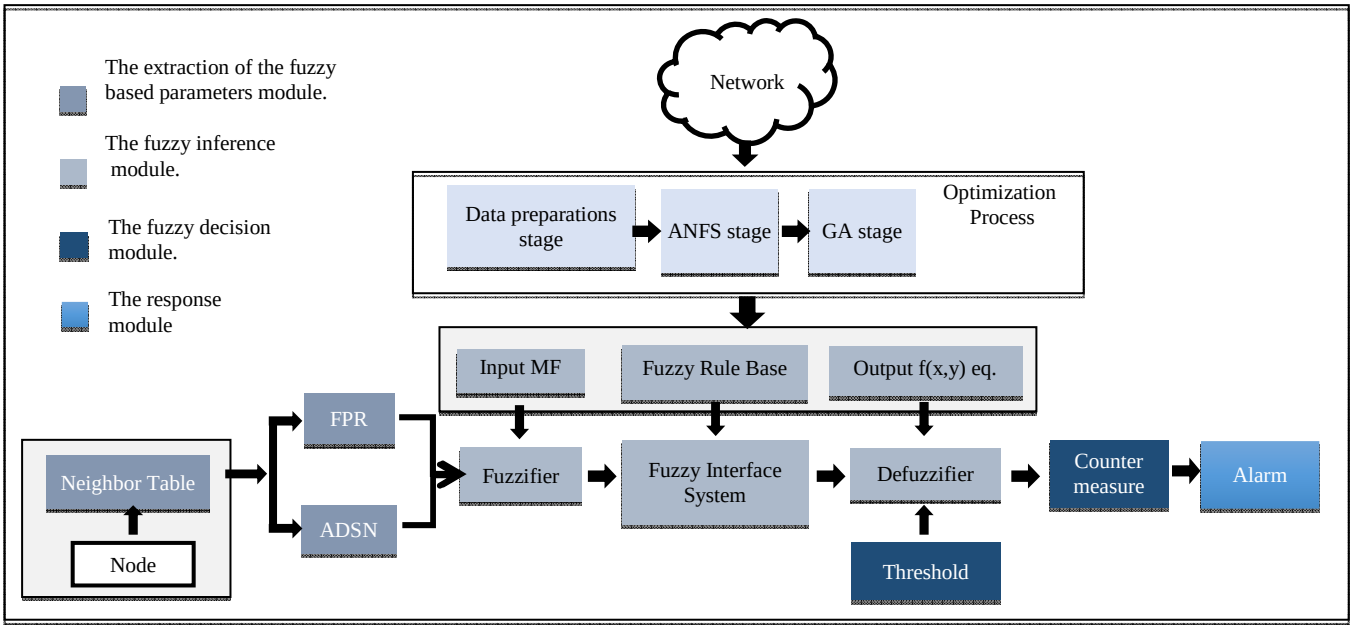

Figure 4. The optimized proposed system

simulation time	module no.	node IP	neighbor IP	no of packets send by the neighbor	no of packets send to neighbor	ADSN	FPR	desired output
225.3088843	2	10.0.0.67	10.0.0.52	224	472	2	0.474576	10
225.3187703	7	10.0.0.53	10.0.0.52	22	41	5	0.536585	10
225.3200186	7	10.0.0.53	10.0.0.66	59	118	0	0.5	10
225.3219711	9	10.0.0.51	10.0.0.21	1	1388	44	0.00072	0
225.328237	7	10.0.0.53	10.0.0.21	1	1	44	1	10
225.330388	9	10.0.0.51	10.0.0.21	1	68	80	0.014706	0
225.3344127	2	10.0.0.67	10.0.0.15	46	86	4	0.534884	10
225.3377508	2	10.0.0.67	10.0.0.40	80	129	4	0.620155	10
225.3378207	7	10.0.0.53	10.0.0.73	91	186	0	0.489247	10
225.3440355	20	10.0.0.40	10.0.0.21	1	96	43	0.010417	0
225.3461097	2	10.0.0.67	10.0.0.4	180	355	0	0.507042	10
225.359133	53	10.0.0.6	10.0.0.44	44	91	0	0.483516	10
225.3619182	38	10.0.0.59	10.0.0.6	36	53	0	0.679245	10

Figure 5. A snapshot of a sample of database

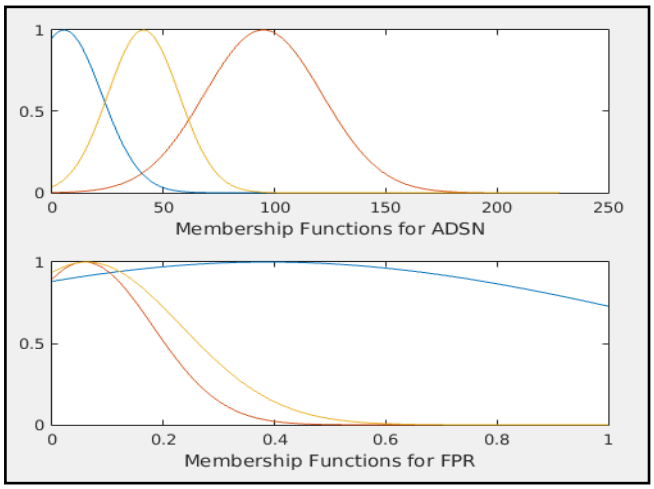

Figure.6 The membership function for initial FIS

After the data mapping process, the input parameters FPR and ADSN must be calculated from the database as explained earlier so we would have three sets of data the FPR set and ADSN set which represented the inputs sets and the target FL as the output set. The entire sets are divided into two groups training group (two-third of the entire sets) and testing group (one set of the entire group). Then up to the next stage which is the ANFS stage. Figure 5 is a snapshot of a sample of the database.

4.2.2. ANFS Stage

The goal of this stage is the generation of initial individuals to be optimized by the genetic algorithm stage. A Sugeno fuzzy module is chosen in this stage represent and for the MFs a Gaussian function was chosen. Where each input set has three MFs, The reasoning system for Sugeno model was explained earlier. Figure 6 is the membership function for initial FIS.

4.2.3. GA Stage

As mentioned even with the use of ANFS system the resulting fuzzy interface system is not optimum because of the use of ANN, so genetic algorithm was used as an optimization tool. Since the GA deal with chromosomes, the variables should be presented to GA encoded by chromosome. Since each Gaussian MFs has two variables (mean "M" and stander deviation "SD") and each rule has three variables (p_i, q_i, r_i)) the chromosome should look like [26], [27]:

$$M_1\ SD_1\ M_2\ SD_2 \ldots\ldots\ldots\ldots p_1\ q_1\ r_1 \ldots\ldots\ldots p_3\ q_3\ r_3 \quad (2)$$

The initial population of individuals, which called the parent population is evaluating by the fitness function. In this study, the Mean Square Error (MSE) is used as a fitness function, which measures the average of the square of error between the resulting of the GA system and the target actual system. The MSE is defined by the following equation:

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n}(P_i - T_i)^2 \quad (3)$$

Where Pi is the value of from the GA system, Ti is the target value and n is the number of data in the training dataset.
Then the individuals with the maximum fitness function are the ones that will be selected to be used to generate the next generation, which is done by crossover the parent population at a random crossover point then the resulting population is mutated in a small percentage value to generate the offspring. The parent population will then be replaced by the offspring and the same operation that was done on the parent population will be used on the offspring to generate the new offspring. The same process is done repeatedly to obtain the optimized solution, which is the one with the minimum error. GA was started with 25 randomly generated chromosomes,

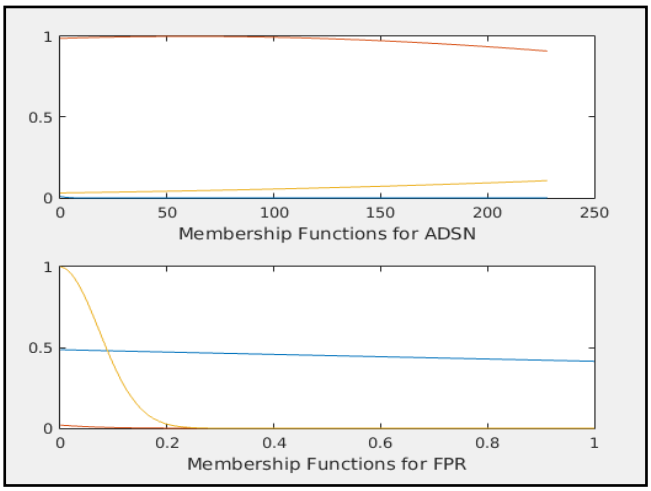

Figure 7. The membership functions for optimized FIS

and their parameters were crossover percentage, mutation rate and population size with the values of 0.4, 0.15, and 25, respectively. Figure 7 shows the optimized membership functions.

5. Performance Evaluation

In this section, we describe the used simulators, simulation methodology, network simulation configurations, and performance metrics.

5.1. Simulators

Three simulators used in this study: OMNET++ simulator version 4.6, which used in the simulation of MANET network, simulation of attack and the IDS. The other simulator was MATLAB, which used in the ANFS stage,

and GA stage in the optimized proposed algorithm, the last simulator used is the QFUZZYLITE, which used to encode the fuzzy interface system into a C++ code to be added into the IDS in OMNET++.

5.2. Simulation Methodology

The network simulated in four situations. Situation (1): The network simulated without the presence of black hole attack. Situation (2): the network simulated with the presence of attack and without the presence of any IDS. Situation (3): the network simulated with the presence of attack and the presence of the normal not optimized intrusion detection system. Situation (4): the network simulated with the presence of attack and the presence of the optimized intrusion detection system. In each situation, the number of source nodes varied from two nodes to twelve nodes. In addition, each situation has two scenarios one with 1m/s mobility and another with 20m/s mobility. The aim of these Scenarios is to see the performance of the network in case of low mobility and high mobility.

5.3. Network Simulation Configurations

The specifications of the proposed network are : (i) Number of nodes: 75 nodes; (ii) Coverage area: 800 × 800 m; (iii) Transport layer: UDP protocol; (iv) Packet length: 512 bytes; (v) Send interval: 0.025s; (vi) Mobility type: Random WP mobility with 15s pause time; (vii) Application layer for source nodes: UDP Basic Burst; (viii) Application layer for intermediate node, destination nodes and attack node: UDP Sink; (ix) Routing protocol: AODV; (x) Mac type: IEEE 802.11; (xi) number of black hole attack: 1; and (xii) Initial position of black hole node: in the center of the network (400,400). Each data point obtained by running the simulation 10 times with different seed numbers and taking the average value.

5.4. Performance Metrics

In this study, two performance metrics used to evaluate the performance of the network in case of AODV with no attack, AODV with an attack, AODV with normal IDS and AODV with optimized IDS. The definitions of those metrics are:

- Packet Delivery Ratio (PDR): This metric shows the ability of the network to successfully deliver packets to the destination, which can be calculated by the ratio of the number of the successfully received packets at the destination to the number of packets sent by the source.

$$\text{PDR} = \frac{\sum \text{No. of packets successfully received at destination}}{\sum \text{no. of packets sent by source nodes}} \quad (4)$$

- Routing Overhead (ROH): This metrics shows how much the intrusion detection system technique overheads the network with packets so it can actually work which can be calculated by the ratio of routing-related packets in bytes (RREQ, RREP, RERR, AACK, IDSRERR) to the total routing and data transmissions (sent or forwarded packets) in bytes. That means the acknowledgments, alarms, and switching overhead is included.

$$\text{ROH} = \frac{\sum \text{routing related packets in bytes}}{\sum \text{total routing/data transmissions in bytes}} \quad (5)$$

In addition, four performance metrics used to test the performance of fuzzy interface system in case of the the FIS from the ANFS stage and the final FIS from the GA stage, which is the optimized FIS. The four performance metrics are Mean Square Error (MSE), Root Mean Squared (RMS), Error Mean, and Error Standard deviation [28].

6. Results and Discussions

In this section, the simulated result presented along with a discussion on this result. The simulation was running on a laptop with processor Core i5 and 4GB RAM with Linux Ubuntu version 15.05 as an operating system. The network simulated in two different scenarios: in low-speed mobility (1 m/s) and high-speed mobility (20 m/s).In each scenario,

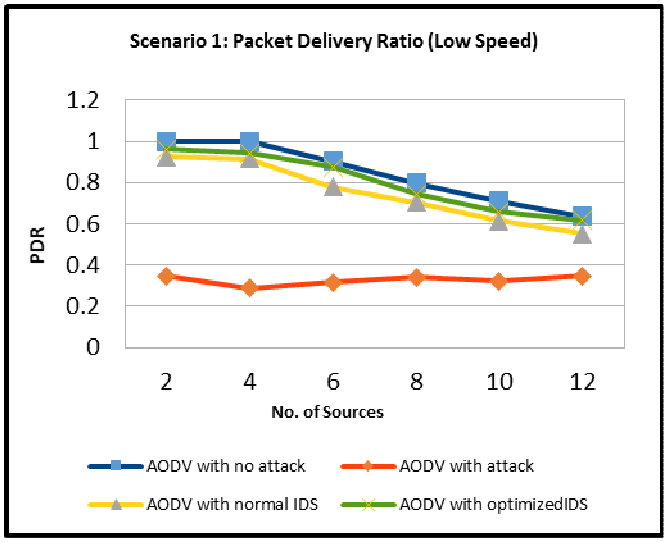

Figure 8. Packet delivery Ration in scenario (1)

the network simulated with different numbers of source nodes from only two source nodes to 12 source nodes, for each one the network simulated in four different situations (without attack, with attack, with normal estimated IDS, and with optimized automated IDS). Each data point obtained by running the simulation 10 times with different seed numbers and taking the average value.

PDR results in low-speed mobility of 1 m/s presented in Figure 8. The delivery of the packets in case of no attack presents the ability of the MANET itself to deliver packets, as seen; with the increase of source nodes, this ability decreased. In the case of two and four source nodes, the PDR is nearly 100% but with an average of 83.9%.In the case of attack, this percentage drops down to an average of 32.6%, this low percentage come from the fact that the black hole node is located in the center of the network so it nearly affects the whole network. However, with normal estimated fuzzy IDS this percentage goes up to 74.8%, which consider low performance, but the optimized automated proposed IDS increases this percentage to be on an average of 80% so it is only 3.9% less from the average percentage of the simulated network in case of no attack. Therefore, from the above results, it is obvious that there is an improvement in the PDR

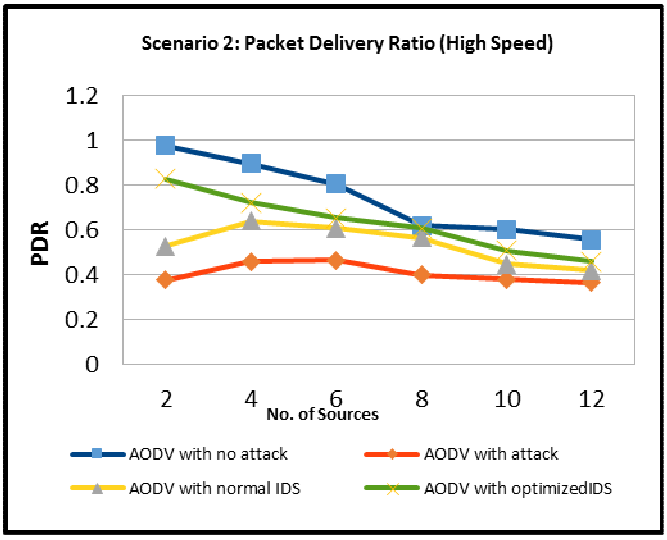

Figure.9 Packet delivery Ration in scenario (2)

by using the optimized automated system by an average of 5.21% from the normal estimated system. Noticing that the three curves (no attack, normal IDS, and optimized IDS curves) are similar in shape and the network with four source nodes or less have the best performance. In addition, from the above result, four source nodes or less seems to have better performance with an average of 95.3% packet delivery.

However, this result is not the same as in high-speed mobility 20 m/s, see Figure 9.The detection effectiveness tends to decrease when the nodes are highly mobile because of the nature of the network as with high mobility the route maintenance packet increased and the success in packet transmission decreased. For high mobility, the average of the PDR for a different simulated network with different no. of source nodes are 74.3% without attack, noticing that from two to six source nodes the PDR have a minimum value of have 80 % but as the sources nodes go up from 8 to 12 source nodes the PDR decreased to an average of 60%. However, with attack this percentage drops down to an average of 40%. But with normal estimated fuzzy IDS this percentage does up to only 53.6%, however, the optimized proposed IDS increases this percentage to be on an average of 63% so it is 11.3% less from the percentage of the simulated network in case of no attack. This is an improvement from the simulated estimated fuzzy IDS but

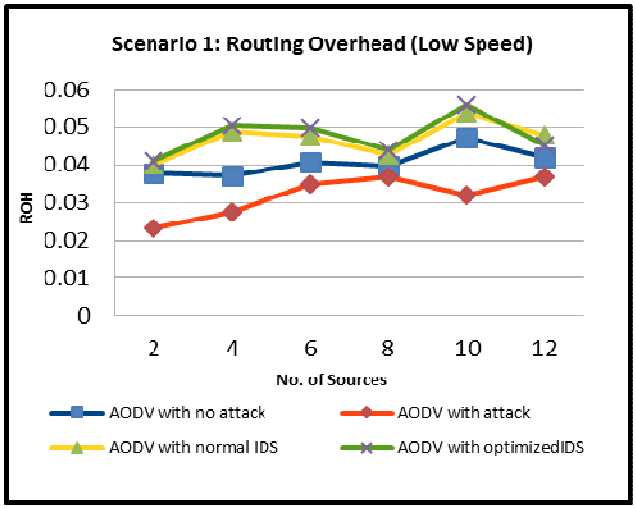

Figure 10. Routing overhead in scenario (1)

still high mobility the performance is low. Noticing that in the case of only two source nodes, this percentage is much higher. Another performance evaluation presented, which is ROH, see Figure 10 for the results in low-speed mobility. As seen, the ROH increased by the use of IDS because of the use of the IDSRERR message, which is used by the detecting node to inform the other nodes about the attack. The average ROH in case of no attack is 4% from the total traffic, this percentage goes down to 3% in case of attack because the

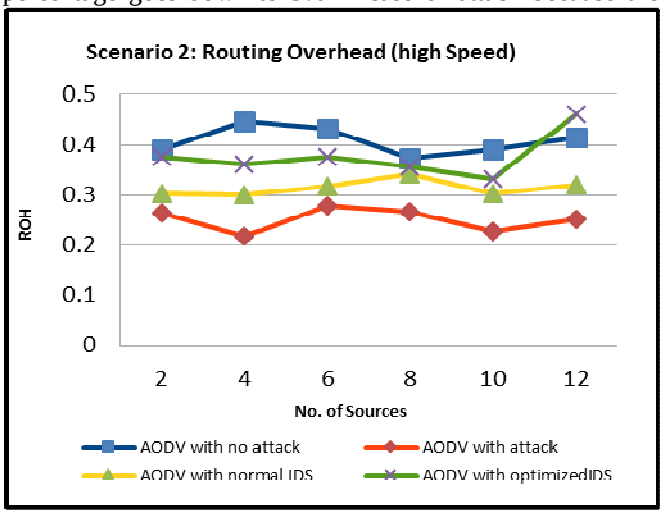

Figure.11 Routing overhead in scenario (2)

route maintenance packet is decreased due to the presence of black hole attack as it manipulate the network to think that it deliver the data packets when in fact it doesn't. The use of the IDSRERR appears in both of the normal estimated IDS and the optimized automated IDS, as for the first the average ROH is 4.6% from the total traffic and for the second 4.7%. Noticing that in all situation, the case if 8 source nodes represents the lowest ROH.

For scenario (2) with high-speed mobility, the ROH takes another shape; see Figure 11. In case of high mobility, the results changed completely due to the route maintenance process with large no of routing messages to maintain transmission between nodes even with high mobility. Noticing that the ROH has its biggest value in case of no attack because the effect of the route maintenance packets appears the most with an average of 4%, in case of normal estimated IDS the percentage is 3% that is due to the effect of black hole attack is still present with only 53.6% packet delivery. However, as the PDR increases in the optimized estimated IDS the ROH also increases with an average of 3.7%.

The performance of FIS in case of the initial FIS from the ANFS stage and the final FIS from the GA stage, which is the optimized FIS, shown in Table 2. Noticing that the GA stage has a good effect on the FIS. From the below results it is proven to say that the use of the proposed IDS provide a mush robust IDS comparing with the estimated IDS. In addition, it is safe to say that the on-demand routing protocols such as the AODV routing protocol has low performance in case of high-speed.

Table 2. The performance of the initial and optimized FIS

Metric / FIS	MSE	RMSE	Error Mean	Error St.D
Optimized FIS	0.3682	0.6068	0.035503	0.60603
Initialized FIS	4.8856	2.2103	0.00447	2.2113

7. Conclusion

Is this paper an optimization of a fuzzy based intrusion detection system is introduced to detect and prevent the effect of a black hole attack. In addition, an estimated (not optimized) fuzzy based intrusion detection system is introduced to see the effect of the optimization on the strength of the system. The estimated one relies on the researcher experience in order to choose the number, shape, and position of the membership function for each fuzzy set. In addition, it requires an effort from the researcher to sets the rule base for that fuzzy system which makes a room for error. In another hand, the optimized system automates and optimizes the process of determining the membership functions and the rule base for the fuzzy engine, which make it easier to emblements the system. The danger of the black hole attack comes from the fact that it swallows the network traffic by sending fake RREP messages. From the above results it is proven to say that the optimized proposed system was improved in an average of 5% from the estimated system in scenario (1) and improved to an average of 9% from the estimated system in scenario (2) in the packet delivery ratio but with an increase of an average of 0.1% in the routing overhead in scenario (1) and an increase of an average of 6% in scenario (2).The simulation results proved that the automated optimized system has good detection effectiveness against the black hole attack but with slightly an increase in the ROH with an average of 0.07% from the ROH of the simulated network in case of no attack in low speed.

References

[1] Y. Kim, R. Evans, and W. Iversen "Remote sensing and control of an irrigation system using a distributed wireless sensor network," IEEE Transactions on Instrumentation and Measurement, vol. 57, no. 7, pp. 1379-1387, 2008.

[2] Khin, Thandar, "Impact of Blackhole Attack on Aodv routing Protocol," International Journal of Information Technology, Modeling and Computing (IJITMC), vol. 2, No. 2, pp. 9-17, 2014.

[3] Sabarish D, and Ranjani C, "Enhanced DSR Protocol for Detection and Exclusion of Selective Black Hole Attack in MANET," International Journal of Computer Applications, vol. 112, No. 14, pp. 32-35, 2015.

[4] P. Gowrisankar, N. Srinivasulu, Ch. Balaswamy, "Design and Implementation of Black-hole Attacks in AODV Routing Protocol for Mobile Ad-hoc Networks," International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, No. 12, pp. 4548-4553, 2013.

[5] Goyal, Priyanka, and et al., "MANET: Vulnerabilities, Challenges, Attacks, Application," IJCEM International Journal of Computational Engineering & Management, vol. 11, pp. 32-37, 2011.

[6] Dyer, J. Perez, Ronald, "Personal Firewalls and Intrusion Detection Systems," The proceeding of 2nd Australian Information Warfare Security Conference IWAR, 2001.

[7] T. Anantvalee,and J. Wu, "A Survey on Intrusion Detection in Mobile Adhoc network," Wireless Network Security, pp. 159-180, US Springer, 2007.

[8] Abasikeleş, "A Realistic Modelling of the Sinkhole and the Black Hole Attacks in Cluster-Based WSNs," International Journal of Electronics and Electrical Engineering, vol. 4, No. 1, pp. 74-78, 2016.

[9] Z. Al-Haddad, M. Hanoune and A. Mamouni, "A Collaborative Network Intrusion Detection System (C-NIDS) in Cloud Computing," International Journal of Communication Networks and Information Security (IJCNIS) Vol. 8, No. 3, pp. 130-135, 2016

[10] O. Eo, E. MM, "A Review of Black Hole and Worm Hole Attack on AODV Routing Protocol in MANET," International Journal of Engineering Trends and Technology (IJETT), vol. 9, No. 8, pp. 394-399, 2014.

[11] M. Wahengbam, and N.Marchang, "Intrusion detection in manet using fuzzy logic," The proceeding of Emerging trends and applications in computer science (NCETACS), pp. 189-192, 2012.

[12] Balan, E. Vishnu, and et al., "Fuzzy based intrusion detection systems in MANET." In Proceeding Computer Science. pp. 109-114. 2015.

[13] Sujatha, R. S. Bhuvaneswaran, and et al., "Design of Genetic Algorithm based IDS for MANET." In Recent Trends in Information Technology (ICRTIT). pp. 28-33. IEEE, 2012.

[14] Kurosawa, Satoshi, and et al., "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method." IJ Network Security. vol. 5, No. 3, pp. 338-346, 2007.

[15] Yunwu, Wang. "Using Fuzzy Expert System Based on Genetic Algorithms for Intrusion Detection System." In Information Technology and Applications. vol. 2, pp. 221-224, 2009.

[16] S. Shamshirband, N. B. Anuar, M. L. M. Kiah, and A. Patel, "An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique," Engineering Applications of Artificial Intelligence, vol. 26, no. 9, pp. 2105–2127, 2013.

[17] S. A. Joshi and V. S. Pimprale, "Network Intrusion Detection System (NIDS) based on data mining," International Journal of Engineering Science and Innovative Technology, vol. 2, no. 1, pp. 95–98, 2013.

[18] M. Govindarajan and V. Abinaya, "An outlier detection approach with data mining in wireless sensor network," International Journal of Current Engineering and Technology, vol. 4, pp. 929–932, 2014.

[19] Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 266–282, 2014.

[20] Biswas, M. Sharma, T. Poddder, and N. Kar, "An approach towards multilevel and multiagent based intrusion detection system," in Proceedings of the IEEE International Conference on Advanced Communication, Control and Computing Technologies (ICACCCT '14), pp. 1787–1790, IEEE, 2014.

[21] P. Ghosekar, G. Katkar and P. Ghorpade, "Mobile ad hoc networking: imperatives and challenges," IJCA Special Issue on "Mobile Ad-hoc Networks", no. 3, pp. 153-158, 2010.

[22] E. E. Khin, and T. Phyu, "Impact of Black hole Attack on AODV routing Protocol," International Journal of Information Technology, Modeling and Computing (IJITMC), vol. 2, No. 2, pp. 9-17, 2014.

[23] P. Tahmasebi, and A. Hezarkhani, "A hybrid neural networks-fuzzy logic-genetic algorithm for grade estimation," Computers & Geosciences, vol. 42, pp. 18-27, 2012.

[24] S. Sahraoui, S. Bouam, "Secure Routing Optimization in Hierarchical Cluster-Based Wireless Sensor Networks,"

International Journal of Communication Networks and Information Security (IJCNIS), vol. 5, No. 3, pp. 178-185, 2013.

[25] J. Singh, and Kulbhushan, "Fuzzy Logic based Intrusion Detection System against Blackhole Attack on AODV in MANET," Computing, pp. 28-35, 2011.

[26] K. Tang, K. Man, Z. Liu, and S. Kwong, "Minimal fuzzy memberships and rules using hierarchical genetic algorithms," IEEE Transactions on Industrial Electronics, vol. 45, No. 1, pp. 162-169, 1998.

[27] K. Shimojima, T. Fukuda, and Y. Hasegawa. "Self-tuning fuzzy modeling with adaptive membership function, rules, and hierarchical structure based on genetic algorithm." Fuzzy sets and systems, vol. 71, No. 3, pp. 295-309, 1995.

[28] Rice, John. “Mathematical statistics and data analysis”. Nelson Education, 2006.