IDS Against Black-Hole Attack for MANET

Mohamed Abd-El-Azim, Hossam EL-Din Salah, and Menas Ebrahim
(Corresponding author: Menas Ebrahim)

Electronics and Communications Engineering Department, Mansoura University
Mansoura 35516, Egypt
(Email: menasebrahim@gmail.com)

(Received Feb. 13, 2017; revised and accepted June 25, 2017)

Abstract

Black-Hole and Gray-Hole attack considers two of the most affected kind of attacks on the Mobile Ad-Hoc Network (MANET). Therefore, the use of intrusion detection system (IDS) has a major importance in the MANET protection. In this paper, a proposed optimized fuzzy based intrusion detection system is presented with an automation 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).

Keywords: ANFIS; Black-Hole Attack; FIS; GA

1 Introduction

Mobile ad-hoc network (MANET) is a new and evolving area of interests, which used in many different applications [6]. The black-hole attack is a Denial of Service (DoS) attack; it works by drawdown packets in the network to a malicious node and then drops, alters the content of the packets, or even passes the packets to another malicious node [1]. Another effective attack is gray-hole attack [7], MANET works under an assumption that all nodes in the network are collaborating to forward packets [3], which is not true as there are selfish nodes that refuse to forward the packets to reserve its energy and other resources, also there are attack nodes, which drop packet to harm the network. One of the important parts in utilizing and deploying the MANET is securing it. Achieving a secure MANET helps this kind of network to achieve its full potential, which is to be used not only in military and crises situation applications but also in a commercial way. A certain level of security can accomplish by using the existing security solution [25]. However, because of the nature of the MANET, it has its own vulnerabilities coupled with the normal vulnerabilities of the wireless networks [5]. Therefore, these solutions cannot provide a sufficient security level. Intrusion detection systems [2] with the traditional security solutions can accomplish a sufficient security level. In this paper, a proposed intrusion detection system (IDS) introduced against the black-hole and gray-Hole attack where an adaptive neuro-fuzzy inference system (ANFIS) used to automate the process of producing a fuzzy system and then optimizes this system using the genetic algorithm (GA). The system tested in the presence of black-Hole attack and the presence of both black and gray-hole attack.

The rest of this paper is organized as follow: Section 2: literature survey; Section 3: problem statement; Section 4: proposed systems; Section 5: performance evaluation; Section 6: results are discussions, and Section 7: conclusions.

2 Literature Survey

There are many techniques used to detect the packet drop attack (mainly black-Hole attack and gray-attack) some of these techniques are presented below [8, 24].

2.1 PDRR Based Detection Method

The packet Drop Ratio (PDRR) used in [19] to detect the behavior of black-Hole nodes. The PDRR calculated from the Packet Delivery Ratio (PDR) where it is used as a performance metric. The maximum PDRR calculated in an attack free network and then sets as a threshold value.

In network exhibiting attacks the PDR calculated for each node, the node that has a PDR exceeds the threshold value consider malicious otherwise, its behavior consider normal.

2.2 Promiscuous Mode Detection Method

A secure routing protocol presented in [21], which is a secure modified version of the ad-hoc on demand distance vector (AODV) routing protocol. In this modified routing protocol, the promiscuous mode used to detect malicious nodes. The promiscuous mode allows any node to overhear the communication of its neighbors. As soon as the tested node sends a route reply (RREP) message to the source node replying to the route request (RREQ) message, its neighbor promiscuously hears this RREP. So, it sent a plane packet to the tested node to see if it forwarded it to the destination if it does the testing node is considered normal and if not malicious.

2.3 Additional RREP Detection Method

In [13], a secure AODV routing protocol presented to detect the malicious nodes by adding a preprocessing stage called preprocess RREP. In this method, all the RREP messages received in a predefined time slot is stored to find the freshest RREP, analyze the data, and secure route to the destination. When the source node receives RREP messages it stores them and compares its destination sequence number, whenever a RREP message received with a much higher destination sequence number the RREP will be discarded and the black-Hole attack is detected.

2.4 Watchdog and Pathrater Detection Method

The watchdog and pathrater technique was introduced by Marti *et al.* in [15]; it was added on top of the standard routing protocol to increase the throughput of the network when malicious nodes appear in the network. This method is divided into two parts: watchdog part and Pathrater part. The watchdog part works as IDS for MANETs to prevent malicious nodes. This is done by promiscuously listening to its next hop's transmission, if the node does not transmit the packet within a predefined time the watchdog increases its failure counter, Whenever a node's failure counter surpasses a predefined limit, the Watchdog hub reports it as getting out of hand. When a node reported as a misbehaving node the pathrater which is the other part of the technique work with the routing protocol to avoid the misbehaving nodes in the future transmission. This technique proved itself efficient; it is also a node detection technique rather than link detection technique.

2.5 Permutation-Based ACK Detection Method

In [9], Dave proposed an Ad-hoc On-demand Multipath Secure Routing (AOMSR), which is an improvement of the AODV routing protocol with a security mechanism based on the adaptive acknowledgment (AACK) and TWO-ACK security mechanism. In this protocol, the source node stores all the paths to the destination that came from the RREP message. After detecting many routes to the destination, the source node sends the same packet throughout those paths. Every time the destination node receives this packet from any of these paths, the destination node sends back a permutated acknowledgment. If one of these paths does not send back a permutated acknowledgment, a black-Hole attack can be detected.

2.6 Using Fuzzy Logic Approach

The fuzzy logic used in intrusion detection since 90's [16] because it is able to deal with uncertainty and complexity, which derived from human reasoning. By the help of fuzzy variables or linguistic terms, intrusion detection features can be viewed easily and the decision of normal and abnormal activity in the network is based on its fuzziness nature that can identify the degree of maliciousness of a node instead of yes or no conditions. IF-then-else based fuzzy rules are used to define all situations in the network for identifying the attacks or intrusions. The fuzzy rule-based system is known as fuzzy interference system (FIS) that is responsible for taking decisions.

Method (1): Ramkumar in [17], proposed a fuzzy based IDS where forward packet ratio and the average destination sequence number is used to distinguish normal from malicious. The system is divided into four parts: (1) Fuzzy factor withdrawal, (2) Fuzzy calculation, (3) Fuzzy confirmation module and (4) Alarm packet generation module.

Method (2): Balan in [4], proposed a 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.

Method (3): Wahengbam in [29] proposed a fuzzy based IDS. The parameters used in work were the number of packets lost and the number of packets forwarded by the node.

Method (4): Sengar *et al.* in [20] proposed a fuzzy based where a trust level is calculated by a proposed formula. Three ranges to this trust level used to categorize the nodes and differ the normal from abnormal behavior.

Method (5): Vydeki *et al.* used in [28] a Sugeno type-2 FIS to detect the black-Hole attack. It is proven to have 97% detection rate.

3 Problem Statement

The black-hole attack is a denial of service attack which drawdown the network traffic to a specific malicious node. The attack node in this type of attack act maliciously in the route discovery process [14], this is done by sending a fake route reply message to a requesting source node when it sends a route request message with a fake destination sequence number to fool the source node that it is the shortest path to the destination. Then it drops, alters the content of the packets, or even passes the packets

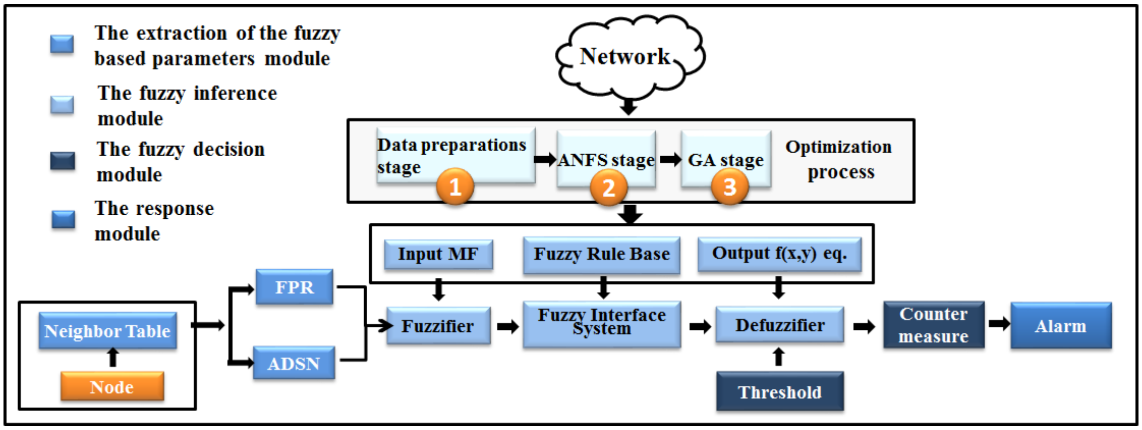

Figure 1: The normal proposed system in detail

to another malicious node. The gray-hole attack is also a denial of service attack like the black-Hole attack. The big difference between the two is that the black-Hole attack act maliciously from the beginning at the route discovery process but the gray-hole attack does not. In gray-hole attack, the malicious node acts legitimately in the route discovery process by sending a true RREP message, but if it is chosen to forward packets is act maliciously [11]. The malicious node can accomplish the gray-hole attack selectively. This can be done by dropping packets for a specific destination, or at a defined part of the day, or by dropping a packet every t seconds or every n packets, or even a randomly selected portion of the packets [18]. To detect the behavior of this attack and prevent it from affecting the network an IDS mechanism must be used.

4 Proposed Systems

In many types of research, the solution of detection the black and gray-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 function 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 and gray-Hole attack a fuzzy based IDS is introduced. A similar optimization process used for grade estimation in [26].

The proposed intrusion detection system illustrated in Figure 1 consists of four main modules: (1) Extraction of the fuzzy based parameters module; (2) Fuzzy inference module; (3) Fuzzy decision module; and (4) Response module. To optimize and automate the fuzzy interface module an optimization process is done which includes three stages: Data preparations stage, ANFS stage, and GA stage.

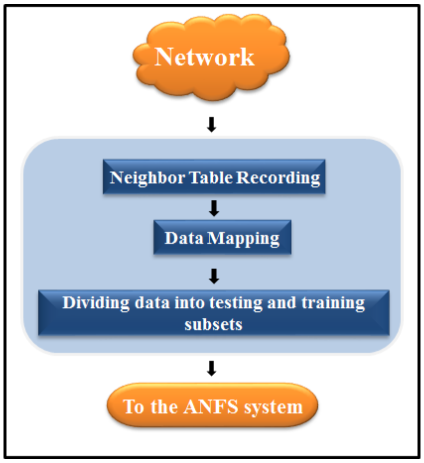

Figure 2: The data preparation stage

4.1 Extraction of Fuzzy Based Parameters

In this module, a set of parameters chosen to be extracted from the network (this parameter should be the most affected parameters when attack nodes are presented in the network); in this system, the forward packet ratio (FPR) and the average destination sequence number (ADSN) are chosen [23] as an input to FIS. In addition, the fidelity level is chosen as an output from the FIS. To do that a neighbor table is presented to every node in the network to be able to store the number of forwarded data packets, the no. of the packets that the neighbor has been sending, and the destination sequence numbers that the node receives from the neighbor each time it sends an RREP message to it. Equation (1) can calculate FPR and ADSN for each neighbor as follows:

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

ADSN for each node calculated by averaging the destination sequence numbers stored in the neighbor table in a predefined time slot.

4.2 Fuzzy Inference Module

An automation process is done to find the number of the membership function for each fuzzy set, the shape, and the position of each one to minimize the error that can be done by setting these parameters manually. To optimize and automate the fuzzy interface module an optimization process is done which includes three stages: Data preparations stage, ANFS stage, and GA stage.

4.3 Data Preparations Stage

A database is extracted from the network by recording all the activity of all the nodes in the network. Then a mapping process is done by mapping the normal activity with high FL (10 is chosen in the system) and the malicious activity with low FL (0 is chosen in the system). In the learning process, the normal activity and the malicious activity is known by the IP address of each node. After that, the input parameters "forward packet ratio" and "average destination sequence number" must be calculated from the database. The entire sets are divided into two groups training group and testing group the first is two-third of the data set and the second is the remaining third. See Figure 2 for the Data Preparations Stage process.

4.4 ANFS Stage

A generation of the initial individuals of the FIS is done in this stage which will be optimized in the GA stage. A Sugeno FIS with Gaussian MFs is chosen in this stage Figure 3 is the MFs for initial FIS. In addition, see Figure 4 for ANFS stage process.

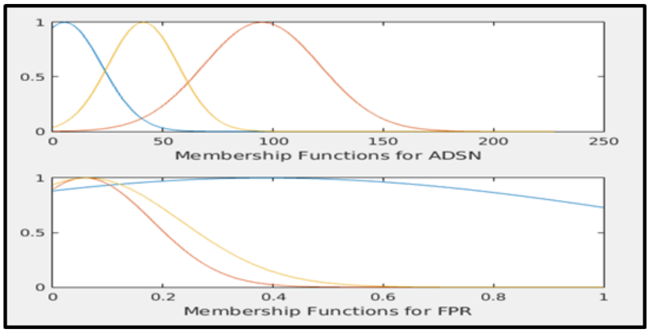

Figure 3: The membership function for initial FIS

4.5 GA Stage

This module used as an optimization tool. Since the GA deal with chromosomes, the variables presented to GA encoded by chromosome. Since each Gaussian MFs has two variables (mean "M" and standard deviation "SD") and each rule has three variables (p_i q_i r_i)) the chromosome should look like, see Equation (1) [22, 27]:

$$M_1SD_1M_2SD_2 \ldots\ldots\ldots p_1q_1r_1 \ldots\ldots\ldots p_3q_3r_3 \qquad (2)$$

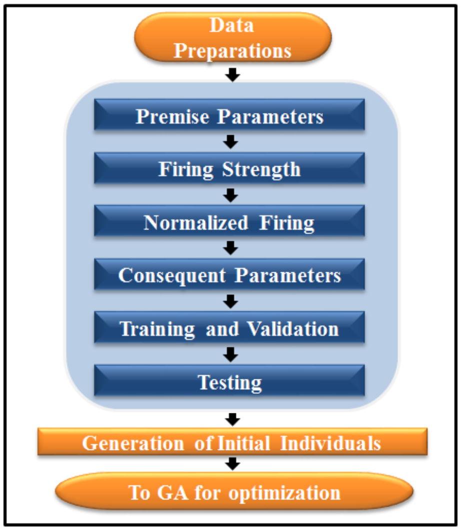

Figure 4: The ANFS stage

The initial population of individuals, which called the parent population is evaluated by the fitness function, which is the Mean Square Error (MSE). See Equation (3):

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

Where P_i is the value of from the GA system, T_i is the target value and n is the number of data in the training dataset. GA started with 25 randomly generated chromosomes, and their parameters were crossover percentage, mutation rate and population size with the values of 0.4, 0.15, and 25, respectively. Figure 9 shows GA optimization process and Figure 9 shows the optimized membership functions.

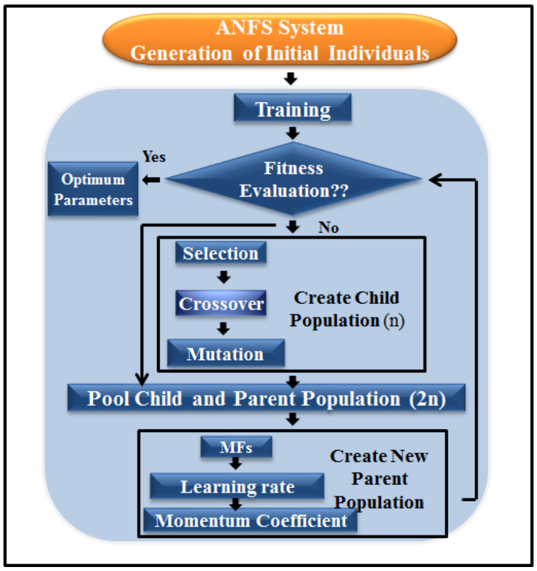
ANFS System
Generation of Initial Individuals
Training
Yes
Optimum Parameters
Fitness Evaluation??
No
Selection
Crossover
Create Child Population (n)
Mutation
Pool Child and Parent Population (2n)
MFs
Learning rate
Momentum Coefficient
Create New Parent Population

Figure 5: The genetic algorithm stage

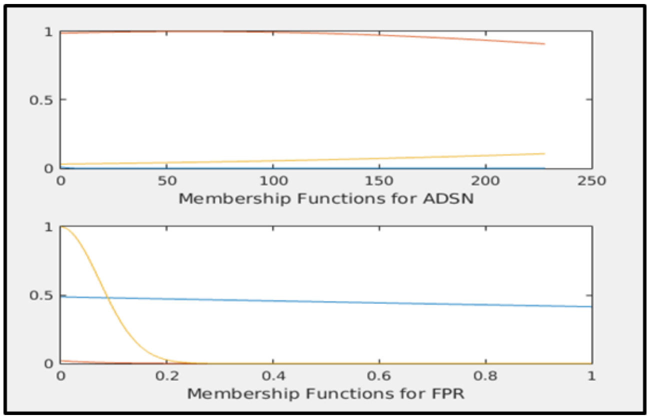

Figure 6: The membership functions for optimized FIS

4.6 Fuzzy Decision Module

A threshold value with three as a value is used in this module to distinguish the normal from the abnormal activity. If the resulted FL from the Fuzzy Inference Module is above the threshold value the node considers legitimate otherwise the node is malicious.

4.7 Response Module

Four actions are done when a malicious node detected:

- Delete the malicious from the routing table.
- Add the malicious node to a blacklist.
- Any route reply message comes from any node in the blacklist considers a fake route reply message and the source nod will not consider it.
- Send a message to the other nodes in the network to inform them about the malicious node.

5 Performance Evaluation

This section describes simulation methodology, network simulation configurations, and performance metrics.

5.1 Simulation Methodology

The network simulated in four situations.Situation (1): The network without the presence of malicious nodes, Situation (2): The network with the presence of only black-Hole node, Situation (3): The network with the presence black-Hole node and gray-Hole nodes, Situation (4): The network with the presence of only black-Hole node and the IDS. Situation (5): The network with the presence of black-Hole node and gray-Hole nodes and the IDS. Each situation simulated with 1 m/s speed mobility and 20 m/s speed mobility

5.2 Network Simulation Configurations

The Network Simulation Configurations presented in Table 1.

Table 1: The network simulation configurations

Parameter Network Parameter	**Value**
Number of nodes	75 nodes
Coverage area	800×800 m
Transport layer	UDP protocol
Packet length	512 bytes
Send interval	0.025s
Mobility type	Random WP
Application layer for source nodes	UDP Basic Burst
No. of sources	2 to 12
Application layer for the other nodes	UDP Sink
Mac type	IEEE 802.11
Routing protocol	AODV
No. of black-hole attack node	1
No. of Gray-hole attack node	10
Initial position of black-Hole node	(400,400)

5.3 Performance Metrics

A number of two performance metrics used to evaluate the performance if the proposed system in the five situations, which are:

- Packet Delivery Ratio (PDR) [12] , which shows the ability to successfully deliver packets to the destination, which can be calculated by Equation (4):

$$PDR = \frac{\sum \text{No.of packets received by the destination node}}{\sum \text{no. of packets sent by source nodes}} \tag{4}$$

- Routing Overhead (ROH) [10], which shows the over heading in the routing related packets resulted by the use of the proposed IDS which can be calculated by Equation (5):

$$ROH = \frac{\sum \text{routing related packets in bytes}}{\sum \text{total routing/data transmissions in byte}} \tag{5}$$

6 Results and Discussions

In this section, the simulated result presented along with result discussion. Two different scenarios presented the first with low-speed mobility (1 m/s) and the second with high-speed mobility (20 m /s). Each scenario simulated in five situations (without attack, with a black-Hole attack only, with both black-Hole and gray-Hole attack, with black-Hole attack and IDS, with both black-Hole and gray-Hole attack and IDS).

The result of the PDR in low-speed mobility presented in Figure 7. The PDR in situation (1) is 99.74% in case of four or fewer source nodes but with an average of 84% in case of twelve or fewer source nodes, which means that the

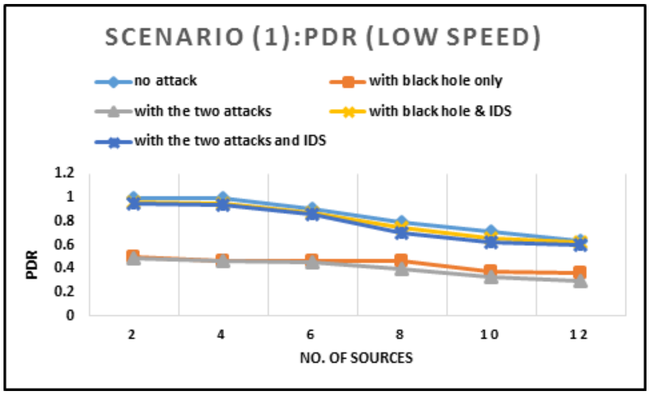

Figure 7: Packet delivery ration in Scenario (1)

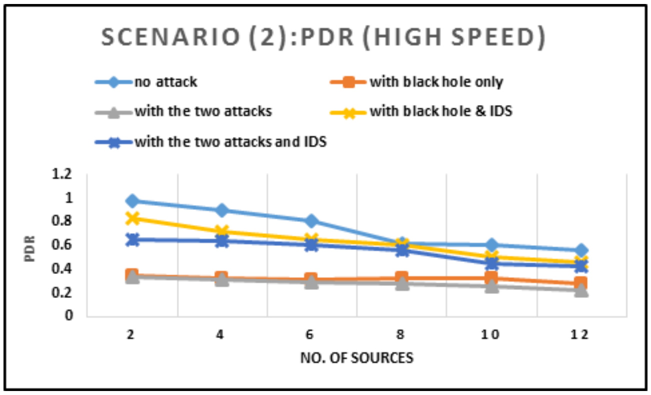

Figure 8: Packet delivery Ration in Scenario (2)

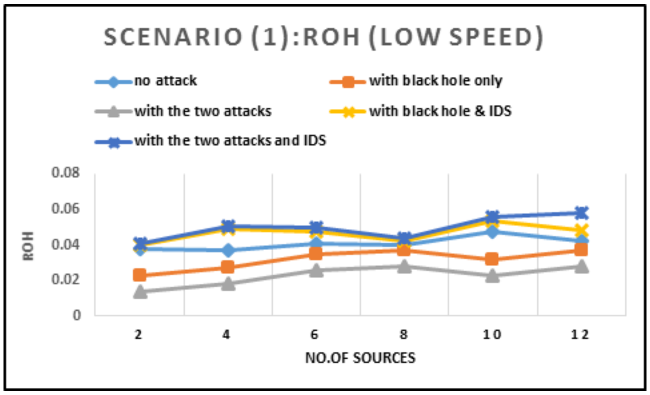

Figure 9: Routing overhead in Scenario (1)

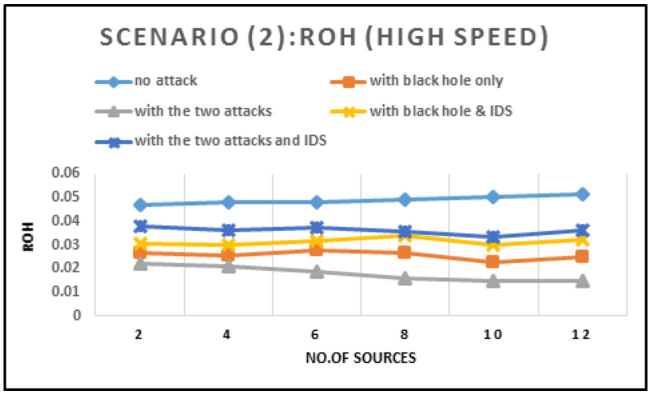

Figure 10: Routing overhead in Scenario (2)

ability to deliver packet decreases with the increase of the number of source nodes. In case situation (2) the average of PDR is 44% but situation (3) the PDR decreases to only 40% which means that the black-hole attack has the big influence on the network. However, with the use of the proposed IDS and the presence of black-Hole attack node, only the PDR increases to an average of 80% with only 4% decrease from the average percentage in case of no attacks. However, this percentage decreases to 78.1% in case of the presence of both attacks, which means that the presence of gray-Hole attack decreases the ability of the system with only 2%.

However, the increase in speed mobility changes the results completely, see Figure 8. The PDR in the case of no attacks is 74.36% in case of four or fewer source nodes but with an average of 93.63% in case of twelve or fewer source nodes. In the case of the presence of a black-Hole node in the network the average of PDR is 31.8% but in the presence of both black-Hole and gray-hole attack node the PDR decreases to only 28.3%. However, with the use of the proposed IDS and the presence of black-Hole attack node, only the PDR increases to an average of 63% with 10% decrease from the average percentage in case of no attacks. In addition, this percentage decreases to 56% in case of the presence of both attacks, which means that in the case of the two attacks and high-speed mobility the system has poor performance.

RoH is another performance evaluation, which presented in Figure 9 with low-speed mobility. The average percentage of RoH in the case of no attack is 4%, which decreases to 3.1% in case of the presences of black-Hole node and decreases again to 3.3 in case of the presence of both attacks this is because of the decrease of the route maintenance packets in the network in the absence of IDS. However, the percentage does up in case of the presences of black-Hole Node and the proposed IDS to 4.7% and to 5% in the presence of both attacks and the proposed IDS because of the use of the IDSRERR message, which is used by the detecting node to inform the other nodes about the attack.

With high speed in Scenario (2) in Figure 10, the RoH changes completely where the highest percentage value of 5% happens in the case of no attacks due to the route maintenance process. Noticing that the value decreases to 2.5% in case of the presence of black-Hole attack only and decreases again to 1.8% in case of the presence of both attacks. In addition, the value goes up again in Situation (4) to 3.1% and increases again to 3.6% when the effect of attacks increases the route maintenance packets.

7 Conclusions

In this paper, a proposed fuzzy IDS presented against both black-Hole and gray-Hole attack. This system depends on an automated process to set the values of the MFs parameter in the fuzzy inference module to prevent errors from setting the parameters values manually. From the simulated results it appears that the black-Hole attack has more influence on the network than the gray-hole attack. It is proven that the network improved with an average of 36% in the presence of black-Hole attack only, and with an average of 37.8% with the presence of both attacks in case of low-speed mobility by using the proposed IDS in the PDR with an increase of 2.5% in the RoH. But in the case of high-speed mobility the network improved with an average of 31% in the presence of black-Hole attack only, and with an average of 27% with the presence of both attacks in case of high-speed mobility by using the proposed IDS in the PDR with an increase of 1.8% in the RoH.

References

[1] I. Abasikeleş-Turgut, M. N. Aydin, and K. Tohma, "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, Feb. 2016.

[2] Y. Altman and A. Y. Keren, *System and Method for Automated Configuration of Intrusion Detection Systems*, US Patent 9,479,523, Oct. 25 2016.

[3] K. Balakrishnan, J. Deng, and V. K. Varshney, "Twoack: Preventing selfishness in mobile ad hoc networks," in *IEEE Wireless Communications and Networking Conference*, vol. 4, pp. 2137–2142, 2005.

[4] E. V. Balan, M. K. Priyan, C. Gokulnath, and G. U. Devi, "Fuzzy based intrusion detection systems in MANET," *Procedia Computer Science*, vol. 50, pp. 109–114, 2015.

[5] G. Banerjee, A. Kumari, A. Thakur, K. Kumari, and J. Parit, "An analysis on characteristics, challenging issues and comparisons of routing protocols of MANET," *International Journal of Scientific Research in Science, Engineering and Technology*, vol. 2, no. 2, pp. 876–879, 2016.

[6] A. O. Bang and P. L. Ramteke, "MANET: History, challenges and applications," *International Journal of Application or Innovation in Engineering & Management*, vol. 2, no. 9, pp. 249–251, 2013.

[7] S. Brar and M. Angurala, "Review on grey-hole attack detection and prevention," *International Journal of Advance research , Ideas and Innovations in Technology*, vol. 2, no. 5, pp. 1–4, 2016.

[8] A. Chaudhary, V. Tiwari, and A. Kumar, "Analysis of fuzzy logic based intrusion detection systems in mobile ad hoc networks," *International Journal of Information Technology*, vol. 6, no. 1, pp. 690–696, 2014.

[9] D. Dave and P. Dave, "An effective black hole attack detection mechanism using permutation based acknowledgement in MANET," in *International Conference on Advances in Computing, Communications and Informatics (ICACCI,14)*, pp. 1690–1696, 2014.

[10] S. Goswami, S. Joardar, C. B. Das, S. Kar, and D. K. Pal, *Performance Analysis of Three Routing Protocols in MANET Using the NS-2 and ANOVA Test with Varying Speed of Nodes*, Ad Hoc Networks, 2017.

[11] M. Gupta and K. K. Joshi, "A review on detection and prevention of gray-hole attack in MANETs," *International Journal of Scientific & Engineering*, vol. 4, no. 11, 2013.

[12] N. Kaur, "Implementing MANET security using CBDS for combating sleep deprivation & DOS attack," *International Journal for Science and Emerging*, vol. 16, no. 1, pp. 6–12, 2014.

[13] V. Khandelwal and D. Goyal, "Blackhole attack and detection method for AODV routing protocol in MANETs," *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 2, no. 4, pp. pp. 1555–1559, 2013.

[14] T. Link and B. D. Gadong, "Performance analysis of MANET under black hole attack using AODV, olsr and tora," in *Computational Intelligence in Information Systems: Proceedings of the Computational Intelligence in Information Systems Conference (CIIS'16)*, vol. 532, Springer, pp. 198, 2016.

[15] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of ACM the 6th Annual International Conference on Mobile Computing and Networking*, pp. 255–265, 2000.

[16] D. J. Norris, "Fuzzy logic system," in *Beginning Artificial Intelligence with the Raspberry Pi*, pp. 111–143, 2017.

[17] J. Ramkumar and R. Murugeswari, "Fuzzy logic approach for detecting black hole attack in hybrid wireless mesh network," in *2014 IEEE International Conference on Innovations in Engineering and Technology (ICIET'14)*, vol. 3, pp. 877–882, 2014.

[18] D. Sabarish and C. Ranjani, "Enhanced DSR protocol for detection and exclusion of selective black hole attack in MANET," *International Journal of Computer Applications*, vol. 112, no. 14, 2015.

[19] S. T. P. Saurabh, "A PDRR based detection technique for blackhole attack in MANET," *International Journal of Computer Science and Information Technologies*, vol. 2, no. 4, pp. 1513–1516, 2011.

[20] M. Sengar, P. P. Singh, and S. Shiwani, "Detection of black hole attack in MANET using fbc technique," *International Journal of Emerging Trends & Technology in Computer Science*, vol. 2, no. 2, pp. 269–272, 2013.

[21] G. Sharma and M. Gupta, "Black hole detection in MANET using AODV routing protocol," *International Journal of Soft Computing and Engineering*, vol. 2, 2012.

[22] 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.

[23] J. Singh, "Fuzzy logic based intrusion detection system against blackhole attack on AODV in MANET," *IJCA Special Issue on Network Security and Cryptography*, pp. 28–35, 2011.

[24] M. M. Singh, A. Singh, and J. K. Mandal, "A snapshot of black hole attack detection in MANET," *International Journal of Computer Applications*, vol. 116, no. 14, 2015.

[25] R. Singh and D. Kumar, "MANET: Security issues and behavior analysis of routing protocol using NS-2," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, no. 4, 2015.

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

[27] K.-S. Tang, K.-F. Man, Z.-F. 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.

[28] D. Vydeki and R. S. Bhuvaneswaran, "Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks," *Journal of Computer Science*, vol. 9, no. 4, pp. 521–525, 2013.

[29] M. Wahengbam and N. Marchang, "Intrusion detection in MANET using fuzzy logic," in *3rd national conference on Emerging trends and applications in computer science (NCETACS'12)*, pp. 189–192, 2012.

Biography

Mohamed Abdel-Azim received the Ph.D. degree in Electronics and Communications Engineering from the Faculty of Engineering-Mansoura University-Egypt by 2006. After that he worked as an assistant professor at the electronics & communications engineering department, then awarded the associate professor degree in 2012 until now. He has 130 publications in various international journals and conferences. His current research interests are in multimedia processing, wireless communication systems, and field programmable gate array (FPGA) applications. He had awarded the best Ph.D. thesis at Mansoura University at 2007. He is the executive director of scientific computing center and the consultant for IT in Mansoura University.

Hossam El-Din Salah, associated professor at electronics and communications department -Faculty of Engineering - Mansoura University, BSc of electronics from Faculty of Engineering - Mansoura University 1993, MSc of electrical communications engineering Faculty of Engineering - Mansoura University - 2000, PhD of electrical communications engineering Faculty of Engineering - Mansoura University - 2008.

Menas Ebrahim received the Master degree in Electronics and Communications Engineering from the Faculty of Engineering-Mansoura University-Egypt by 2017. She worked as a Teaching assistant at the electronics& communications engineering department in MISR Engineering & Technology higher institute since 2012.