An Enhanced Cross-Layer Approach Based on Fuzzy-Logic for Securing Wireless Ad-Hoc Networks from Black Hole Attacks

Mohammad M. Shurman[1*], Omar M. Al-Jarrah[2], Salem B. Esoh[3], Sharhabeel H. Alnabelsi[4]

[1]Network Eng. and Security Dept., Jordan University of Science and Technology, Irbid, Jordan
[2]Computer Eng. Dept., Jordan University of Science and Technology, Irbid, Jordan
[3]Computer Eng. Dept., Jordan University of Science and Technology, Irbid, Jordan
[4]Computer Eng. Dept., Faculty of Eng. Technology, Al-Balqa Applied University, Amman, Jordan

[1]alshurman@just.edu.jo, [2]aljarrah@just.edu.jo, [3]salem_esoh@yahoo.com, [4]alnabsh1@bau.edu.jo

Abstract – *Black holes attack in wireless ad-hoc networks can obstruct network functions, e.g.; successful packets delivery ratio to destinations. Current conventional detection mechanisms are based on single layer information, lack of appropriate performance metrics, and/or the adequate accuracy. In this paper, a new cross-layer Intrusion Detection System (IDS) is proposed, in order to mitigate the black hole attack in wireless ad-hoc networks. The proposed work modifies ad-hoc routing protocol for black hole attacks detection through extracting information from different OSI layers, and use these information as inputs into the fuzzy logic system, in which the algorithm precisely detects existing malicious nodes. Using NS2 simulation tool, a comprehensive simulation is conducted in order to compare our proposed approach performance with a recent cross layer-based approach for black hole intrusion detection [33]. Simulation results reveal that our proposed system has a tremendous accuracy in detecting black holes with an acceptable additional overhead. Our proposed IDS outperforms studied IDS in [33] in terms of successful packet delivery ratio (PDR).* ***Copyright © 2017 Praise Worthy Prize S.r.l. - All rights reserved.***

Keywords: *Black Hole Attack, Cross-Layer, Fuzzy Logic, Intrusion Detection System, Security, Wireless Ad-hoc Networks.*

Nomenclature

Acronym	*Description*
AI	*Artificial Intelligence*
IDS	*Intrusion Detection System*
PDR	*Packet Delivery Ratio*
FP	*False Positive Rate*
FN	*False Negative Rate*
Fb	*Number of clean nodes wrongly detected as black holes*
Tc	*Number of clean nodes truly detected as clean nodes*
Fc	*Number of black holes wrongly detected as clean nodes*
Tb	*Number of black hole nodes truly detected as black holes*
DR	*Detection Rate*
R	*Residual energy*
C	*Collision*
D	*Dropped packets*
B	*Buffer overflow*
P	*Pause time*
BH	*Black Hole*

I. Introduction

Wireless networks in general are defined as a group of independent devices that communicate with each other wirelessly [1]-[4].

. Wireless networks are gaining more popularity in communication systems during recent years[5]-[6], due to their preferable properties over other types of networks, such as the absence of physical media channels, having no centralized control over the network, and support of mobility, especially, as in wireless ad-hoc networks [7]-[11]. Nevertheless, these aforementioned advantages introduce few shortcomings that might limit wireless networks utilization and make it unsuitable under some conditions. The most crucial challenges are security, power consumption, and quality of service (QoS) assurance [12-15]. In this work, a new cross-layer design is proposed in order to tackle black hole security problem, because these days security challenges are getting more attention.

Ad-hoc networks are the type of wireless networks that used for connecting a group of nodes without the need for a network fixed infrastructure, sometimes called dynamic network. This infrastructure-less style makes wireless

Manuscript received and revised xx 2017, accepted xx 2017
** Corresponding author.*

networks deployment much easier and remarkably with less cost. Wireless ad-hoc networks are the most preferable type of networks for many applications, such as military, emergencies, especially during natural disnatures.

Ad-hoc networks are subject to a large number of security threats, especially, black hole attacks have been one of the most common attacks. That is due to the vulnerabilities found in ad-hoc networks, e.g.; absence of trusted party within the network to ensure the honesty of each node. Despite of the enormous number of approaches that proposed to mitigate the black hole attack during recent years, more work is still needed to improve detection processes of these approaches, e.g.; having high false positive rate (when considering a legitimate node as a malicious one) may affect network performance severely, since higher number of legitimate nodes are depraved from connecting the network. Furthermore, false negative rate is another problem facing the IDS models, where black holes will pass through the IDS without setting off the IDS's alarm, and therefore, this black hole keeps conducting its malicious activities.

Most common attack types in wireless ad-hoc networks domain are the black hole attack [16], wormhole [17] and denial of service [18]. These attacks are mitigated through various techniques like Intrusion Detection System (IDS), encryption and secure routing protocols. A node is considered as a black hole when it prohibits the incoming data from a legitimate sender to be successfully forwarded and transferred to the designated destination [19], e.g.; drop received packets. Black hole attack is a very serious problem in ad-hoc networks where it severely exposes routing protocols performance, such as famous AODV routing protocol, in which AODV is altered and make it impossible for most or even all transmitted packets to be delivered to their designated destination. Consequently, the network is paralyzed and networks' QoS is severely affected [20].

This attack is hard to detect, because the nature of the ad-hoc networks makes it extremely difficult to distinguish between malicious event (black hole attack) and innocuous one (link breaking between nodes, e.g.; due to battery outage for some intermediate nodes). A tremendous work has been conducted, in order to enhance security that assures data delivery to its legitimate-receiver nodes. Researchers introduced different protocols, in order to solve the aforementioned security issues. Some of these solutions are based on a single network layer, where caused overhead delay and operation accuracy still need more improvement [21]-[23].

However, our proposed cross-layer intrusion detection system is based on features that extracted from four different network layers within the standard OSI model. These features are employed as inputs to the fuzzy logic system, where results show a high precision when detecting or classifying black hole nodes and normal nodes. Using our proposed classification system allows excluding black hole nodes, in addition to increasing packet delivery ratio (PDR). Nevertheless, an acceptable increase to the End-to-End (E2E) delay occurs, due to an additional processing time caused by employing our proposed cross-layer classification approach. In this work, we violated the independence of layers which is the sacred principle of OSI model; therefore, more robust IDS can be developed.

In this work, an Artificial Intelligence (AI) system, specifically, fuzzy logic method is used to distinguish a normal node from a black hole node through cross-layer information which deducted from network's behavior. Furthermore, this work provides answers to the following questions:

- What are crucial network layers that should be considered when building a detection or classification system?
- What are the most effective features that should be extracted from network's behavior?
- Which artificial intelligence system should be used in classifying nodes (normal or black hole) has the best performance?

The main inspiration for this work is due to the substantial need for providing security against black hole attacks in wireless ad-hoc networks, due to their exceptional nature. Therefore, more accurate and robust IDS is required, in order to ensure the maximum security from such attacks. Otherwise, a severe drop in the network performance and efficiency occurs, e.g.; packets drop ratio increases dramatically.

The main reasons which motivate researchers of networks security are as follows:

- The uncertainty nature of wireless environment makes it extremely difficult to find a state-of-art anti-black hole system that can deal with various network scenarios.
- Some IDS models mistakenly detect legitimate nodes as black holes, due to the relatively high false positive rate. However, in our proposed system, the false positive rate is reduced to almost zero. Furthermore, the rate of black holes that pass undetected through the proposed system is reduced in order to increase system accuracy.
- Integrating cross-layer approach within an IDS model makes a tremendous improvement on system accuracy and performance.

The proposed work introduces a black hole cross-layer IDS approach that includes additional layers compared to the existing cross-layer IDSs which considered in literature. Namely, physical, MAC, network, and transport layers, such that from each layer specific features are extracted. A fuzzy logic system is built to accurately distinguish a normal node from a malicious one. Through analyzing the network's behavior in various scenarios, membership functions for the system are built with proper values to insure the least error in decision

making. The system evaluation is conducted under many scenarios and with different evaluation metrics with a comprehensive comparison made between the proposed system and other recent cross-layer black hole IDSs.

The remaining of paper is organized as follows: Section II presents related work. The proposed approach is explained in section III. Section IV presents performance metrics of our proposed approach. Section V demonstrates simulation results and their insights. Finally, section VI discusses conclusions and future work.

II. Related Work

The high importance of the security aspect in wireless networks has opened the door for many proposals to insure the highest possible degree of security. Black hole attack is one of main concerns for researchers, and therefore, many countermeasures for this kind of attack are studied.

Two techniques that eliminate black hole problem are proposed in [23]. First technique is to establish an additional redundant route to the same destination from the source node, such that the source node receives multiple acknowledgement packets from two nodes, the actual destination node and the black hole node. However, the source node will only respond to the legitimate route and discard the other malicious route. The second technique is to have an additional table on every node, in order to store information about the last established route. The sequence number of the new route is compared with the legitimate route stored earlier in the additional table. The new route is established only if its sequence number complies with the previous one stored in the additional table. In spite of the good results claimed by these techniques, there are some shortcomings caused by the additional tables that are required for storing routing information, and consequently, this becomes a burden over wireless ad-hoc system due to the fact that memory and power resources in such ad-hoc networks are limited.

Banerjee et al. [24] have proposed an approximate approach to the unique sequence number which is also proposed in [23]. Nevertheless, this method has proven its defects in how to find a standard way to generate a sequence number that is unique and could be used in various scenarios and situations.

Jaisankar et al. [25] have proposed an approach to use the next hop mechanism for securing the network by only modifying the AODV routing table, in which a new field is added among other conventional fields. Furthermore, two new tables are added to the AODV protocol: First table is the Black Identification Table (BIT). Second table is the Isolation Table (IT). The BIT contains these following fields: Source, Target, Current Node ID, Packet Received Count (PRC), Packet Forwarded Count (PFC) and Packet Modified Count (PMC). These fields are used to keep track of the information from nodes and compare them to the information inside the AODV`s conventional routing table, such that if a node has different expected routing information, thereby this node is added to the IT table. As a result, all other nodes consider nodes in IT table as malicious nodes and never respond to them.

Tamilselvan et al. [26] have proposed a new approach by introducing the notion of "fidelity level" variable. This variable represents the extent of trust between nodes, such that transmitting node increments fidelity variable for a neighbor node that really has transmitted packets to the destination. A node with a zero fidelity variable is considered as a black hole, and therefore, removed from network. A similar approach is proposed in [27], in which every node broadcasts a route request to establish a route, and then gather opinions about other nodes that reply to the route request ping, in order to decide whether a certain node is a normal or a malicious node. However, this method has the same shortcoming as the proposed approach in [26].

Authors of [28] have proposed a Time to Live (TTL) based approach, in order to eliminate nodes that do not reply before a certain pre-defined time-threshold. When a route request is sent from a source node and the time-threshold for this request expires before reply packet is received, therefore, the source node considers the next hop node as a malicious one and eliminates it. To develop this protocol, authors modified AODV protocol by inserting a new timer at every route request. This approach has an obvious downside which is the difficulty in finding the optimal value of TTL, especially in dynamic networks, e.g.; ad-hoc networks, where TTL varies or tuned based on network topology.

In [29], an Intrusion Detection using Anomaly Detection (IDAD) is proposed; in which authors consider that every malicious node can be monitored by detecting anomaly behaviors. This system has a pre-collected data, named audit data, which has all odd features and behaviors of a black hole node stored in a database. The network is constantly monitored, such that all behaviors are compared to the already stored audit data features. Consequently, when a specific behavior matches a feature in audit data, the corresponding node is considered as a malicious one and it is immediately isolated.

Another approach called collaborative IDS is proposed by authors in [30], such that instead of forcing every node in the network to perform the IDS operation that requires a lot of processing power and time delay, a collaborative IDS model is proposed. This approach avoids all unnecessary repetitive IDS detections for the same node. If a decision is made for a node, then all other ongoing detection operations for this node are terminated.

In [31], authors proposed one of the first cross-layer design schemes that detect the black hole attack. Each node preserve a new buffer for the next hop neighbor only and not for all neighbors within its range. Furthermore, each node calculates the rate of collision in every transmission. In this case, information from network and MAC layers is observed to develop a cross-layer approach, called detecting black and gray hole

attacks in Mobile Ad-hoc Networks (MANET).

Another cross-layer design method based on authentication is proposed in [32] and called Cross-Layer Based Detection and Authentication in Secure Routing in MANET (CLDASR). Different layers from the OSI model are utilized such as network and MAC layers, in order to gather information about the network and detect whether there is a malicious behavior. Application layer is used to perform secure hashing between source node and application node, in order to avoid the impersonating attack.

A cross-layer approach is proposed in [34] that detects black holes in MANETs. This approach is based on both MAC and network layers within a distributed manner under AODV protocol. It employs Request-to-Send Clear-to-Send (RTS/CTS) control packets, in order to verify nodes legitimacy whether it is a normal or black hole. Based on the fact that black hole node does not has routing information knowledge, therefore, when the black hole receives a route request (RREQ) packet cannot reply with a valid routing information within CTS packet.

Two cross-layer detection methods are developed in [35], where control information is exchanged between three layers. The first method uses information from network and physical layers, such that normal nodes are assigned to a signature key used when transmitting packets. The second method utilizes information from network, MAC, and physical layers, in which a watchdog scheme, developed at network layer, monitors exchanged RTS/CTS packets at MAC layer. Whenever the watchdog overhears CTS from a node and this node does not forward the received packets, therefore, this node is clearly a black hole due to dropping received packets intentionally.

A secure cross-layer routing technique for MANET is proposed in [36]. The detection strategy is based on AODV protocol and honeypot notion, in order to detect and eliminate black hole nodes. The key idea is the honeypot detection module broadcasts a fake RREQ message contains a non-existent source node ID. If any node replies to this packet request, thus this node is considered as a black hole. Note that a normal node does not reply to this fake message, because the fake source node ID does not exist within their routing information.

A novel IDS cluster-based strategy is proposed in [37] that chooses cluster heads in MANETs. Choosing cluster heads aims to reduce energy consumption caused by malicious node monitoring process, where cluster heads selection is conducted by employing Vickrey–Clarke–Groves auction method. A state-of-art method is developed in [38] which detects a cooperative black holes attack for AODV protocol. The “true-link” notion is introduced, which defeats this kind of attack. True-links are constructed based on rendezvous stage, in which links between normal nodes are authenticated.

In 2015, a comprehensive study for one hundred publications about features selection that detect malicious nodes is presented in [39]. Also, authors of [40], [41] have studied many machine learning algorithms, such as neural networks and decision tree that detects gray holes and black holes, in addition to flooding attack.

To detect black hole in Vehicular Ad-hoc Network (VANET), authors in [42] proposed a new routing protocol that prolongs the life time of AODV selected routes by removing detected black holes. Malicious nodes are discovered based on their misbehavior activities, e.g.; transmitting RREP packets to source node with higher sequence number, thus, it is likely this node is a black hole.

A cross-layer IDS approach for mobile ad-hoc networks which is based on features selection is developed in [33]. This approach is designated to mitigate the black hole attack in wireless ad-hoc networks through a cross-layer method. This work is the closest to our proposed work in this paper. Utilized layers in [33] approach are network and MAC layers only. From those two layers, features are extracted to make the system able to distinguish an attack from a normal behavior. However, in our work, features from four network layers are utilized, as explained in section III and shown in Table I.

The main contribution of [33] is the implementation of feature selection process in two different techniques. The first technique, the Rough Set Theory (RST) [43] which is a data mining technique that deals with vagueness and uncertainty of data. The second technique is based on a Genetic Algorithm (GA) [44]. In both techniques, the Support Vector Machine (SVM) classifier separates the attacking behaviors from normal ones. Results show an excellent improvement on the accuracy of the system, especially when implementing GA. However, it is well known that the GA requires high computational power and processing time delay, keep in mind that ad-hoc networks have limited resources, such as memory and power. However, our proposed work yields more detection accuracy with an acceptable additional time delay.

III. The Proposed Approach

In this section, we demonstrate our proposed system which can efficiently detect black holes in wireless ad-hoc networks. The proposed system is comprised of three stages, as shown in figure 1. In the first stage, data is collected for the network and required features are extracted which are rendered to the next stage. The second stage rendered features are used as an input for the fuzzy logic system to be processed. The main purpose of the second stage is to detect whether the node is black hole or normal node using fuzzy theory. In the final stage, a decision about a particular node is taken, whether to

keep this node or to eliminate it because it is a black hole attack.

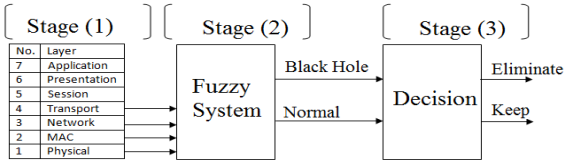

Figure 1: Stages of the proposed system.

TABLE I
NETWORK LAYERS AND THEIR CORRESPONDING UNIQUE STUDIED FEATURES.

Layer Name	Unique Features
Physical	*Total Residual Energy and Mobility*
MAC (Medium Access Control)	*Collision*
Network	*Dropped Packets*
Transport	*Buffer Overflow*

Now, let's explain in details the three stages of our proposed system that is shown in figure 1 as follows:

III.1. Stage 1

The proposed system's robustness relies on the information deduced from the targeted network layers. Therefore, this stage represents layers from which information about network's unique features are extracted. These four layers are physical, MAC, network, and transport layers. However, authors in [33] considered only two layers' features which are MAC and network layers. In this work, the considered features are listed in Table I. Let's explain these five features in details as follows:

1) Total Residual Energy:

Wireless nodes that form ad-hoc networks have limited resources, especially energy where a permanent power source does not exist, and therefore, each node is mounted with a limited lifetime battery. Energy is consumed by a node in various ways such as data processing, transmission, environment sensing and mobility. In this work, the energy consumption is monitored by measuring the amount of residual energy at each node and utilizing this information in detecting black hole nodes. It is assumed that a black hole node consumes more energy than a normal node, apparently, because it is more active than other nodes within the same time period. As a result, black hole node's residual energy must be less than normal nodes.

2) Mobility:

As a fact, mobile nodes do not perform as efficient as fixed nodes, due to their movement while operating. Therefore, it is crucial to consider mobility, because this feature plays a major role in designing an efficient IDS. In other words, as a fact, mobile nodes are more prone to drop more packets than fixed nodes or nodes with less mobility. This feature contributes in classification accuracy between normal and malicious nodes. Clearly, if a fixed node is dropping packet more than neighboring mobile node, thereby this implies this fixed node may be is a black hole.

3) Collision:

Due to the nature of shared medium, air, in wireless networks such as ad-hoc networks, the probability of nodes transmitting at the exact same time increases. Therefore, collision occurs and results in dropping or corrupting all transmitted data during collision time. Unfortunately, when IDS is unaware about this type of collision, this behavior is considered as a black hole attack with a high probability.

4) Dropped Packets:

This feature considers the ratio of unsuccessful packet delivery to the successful ones. Black hole attack mainly works on attracting neighboring nodes to send packets through it, and then dropping all these packets when received. Through monitoring the activity of a particular node, it becomes possible to evaluate this feature. Therefore, this feature is very important in detection process for the proposed system, whether these packets are dropped maliciously or innocuously, e.g.; broken links.

5) Buffer Overflow:

Each node has a limited buffer size to store received packets before forwarding them to their destinations. However, when a node's buffer is full, any additional received packet is dropped. Therefore, this feature helps in distinguishing between a node whose buffer is overwhelmed and a malicious node which is just deliberately drops all incoming packets.

III.2. Stage 2

In this stage, called fuzzy system, features that are deduced from stage 1 are inserted into the fuzzy logic engine, in order to be processed within four phases as follows: First phase, extracted features from stage 1 go through the fuzzification, in which these features are transformed into proper linguistic variables. Second phase, the fuzzy inference system is employed, where collected values are applied into the defined "IF/Then" fuzzy rules as in third phase. Finally, the output of the fuzzy inference system goes through the defuzzification to get a final crisp value. In this work, the crisp output should be one of two possibilities; either this node is a "black hole" or "normal" node.

In order to implement the proposed Mamdani fuzzy system model that mitigates the black hole attack in wireless ad-hoc networks. Five network features, shown

in Table I, Residual energy, collision, dropped packets, buffer overflow and pause time (mobility) are collected from wireless nodes, and then, these features are considered as the input to the fuzzy system. The linguistic variables, also known as fuzzy logic operating parameters, are chosen for input parameters, namely: residual energy (R), collision (C), dropped packets (D), buffer overflow (B) and Pause time (P) (notice that P is the opposite of mobility), and one linguistic variable is chosen for output, namely black hole (BH).

The linguistic variables' ranges, values, membership functions, and the associated values for each parameter are explained in details in the Appendix. Rules for the fuzzy logic system are designed in a way that enhances black hole attack detection accuracy. For example, the following are some of fuzzy rules as in scenario I:

Rule 1: If R is High, then BH is Normal node.
Rule 2: If R is High and D is Low, then BH is Low.
Rule 3: If C is High and D is High, then BH is Low.
Rule 4: If C is Low and D is High, then BH is High.
Rule 5: If B is under and D is High, then BH is High.
Rule 6: If B is under and D is Low, then BH is Low.
Rule 7: If P is Low and D is Medium, then BH is Low.
Rule 8: If P is High and D is High, then BH is High.
Rule 9: If R is Low and C is Low and D is High, then BH is High.
Rule 10: If R is Low and P is High and D is High, then BH is High.
Rule 11: If R is High and C is High and D is High, then BH is Low.

For example, rule 1 means that if residual energy (R) is high, this implies this node is normal. Notice that in rule 6, buffer (B) is "under" implies that buffer overflow did not occur. Also, notice that the parameters of the fuzzy system (such as the number of membership functions and their shapes, linguistic variables ranges and values) and fuzzy rules are initially set based on initial knowledge, however, later they are modified through a tuning stage several times before getting stabilized.

III.3. Stage 3

After nodes honesty is determined in the second stage, an action is required towards these nodes. Therefore, a node which is considered as a black hole must be eliminated from the network, in other words, it becomes isolated such that nodes do not transmit packets to this node. However, if the node is classified as a normal node, thus no action is required against this node.

IV. Performance Metrics for the Proposed System

In order to prove the vitality of the proposed approach, the following performance metrics are used to evaluate studied wireless network.

a) Packet Delivery Ratio (PDR): is the ratio of the number of delivered packets to the total number of all transmitted packets [45], equation (1).

$$PDR = \frac{PD}{Pt} \tag{1}$$

Such that, PD: number of packets delivered to the designated destination successfully. Pt: total number of transmitted packets.

b) False Positive Rate (FP): is the ratio of number of clean nodes that detected as black holes to the total number of the actual clean nodes in network [33], equation (2).

$$FP = \frac{Fb}{Fb + Tc} \tag{2}$$

Such that, FP: False Positive Rate. Fb: Number of clean nodes wrongfully detected as black holes. Tc: number of true clean nodes that detected as clean.

c) False Negative Rate (FN): is the ratio of number of black hole nodes detected as clean nodes to the total number of actual black hole nodes in the network [33], equation (3).

$$FN = \frac{Fc}{Fc + Tb} \tag{3}$$

Such that, FN: False Negative Rate. Tb: Number of true black hole nodes detected as black hole. Fc: Number of black hole nodes wrongfully detected as clean.

d) Detection Rate (DR): is the ratio the total accurate detections to the total detections [33], equation (4).

$$DR = \frac{Tb + Tc}{Tb + Tc + Fb + Fc} \tag{4}$$

e) End-to-End (E2E) Delay: average time required for packet transmission from the source node to the destination node, in addition intermediate nodes transceivers' processing time and the processing time that consumed by the employed IDS.

V. Simulation Results and Discussion

The proposed approach is compared with a closely related system, using the well known network simulator, NS2, to evaluate its performance. The cross-layer features are extracted from four different layers that represent the input to the fuzzy logic system. To get optimal results, the proposed system is simulated in three different scenarios. Each scenario has a specific number of membership functions for the fuzzy logic system, sample of these membership function are presented in the Appendix.

MATLAB software is used for simulating the fuzzy logic system for these three different scenarios, which

allows having the least and the most effective number of fuzzy rules.

V.1. Black Hole Attack

Figure 2 demonstrates a simple black hole attack scenario in an ad-hoc network that consists of five nodes: A, B, C, D and E, such that node D is the black hole attacker, node A is the source node, and node E is the destination node. At the beginning, assume that node A establishes a route through AODV routing protocol by broadcasting a Route Request (RREQ) packet. The attack occurs when the black hole node, node D, replies by a Route Reply (RREP) packet pretending that it has a route to the destination node, node E. Accordingly, nodes C and B re-transmit the RREP packet that transmitted by node D backward to source node, therefore, all packets transmitted to node E are dropped by the black hole (node D).

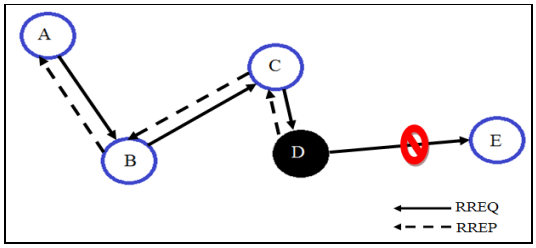

Figure 2: An example of ad-hoc network under black hole attack by node D.

The previous example of the black hole attack, shown in figure 2, is identical to the black hole attack used in our simulation, although our environment contains higher number of nodes. To make thing simpler, in order to seduce other nodes into believing that the black hole has the best route, black hole sends a very high sequence number with the RREP, this technique can be easily detected using a less complicated IDS. However, many attackers use more sophisticated techniques to perform the black hole attack and go undetected through many IDSs.

V.2. Simulation Environment

Network parameters are set to be exact as in [33], therefore, in this way the highest degree of fair comparison is achieved between the proposed approach and the developed cross-layer approach in [33]. Table II shows these parameters used in all simulations conducted using NS2 simulator tool. The simple but powerful Tool Command Language (TCL) is also used, in order to set these parameters for simulated network.

TABLE II
SIMULATED WIRELESS AD-HOC NETWORK PARAMETERS

Parameter	Value
Routing protocol	AODV
Topology	500m*500m
Transmission range	250m
Mobility	Random
Traffic type	CBR/UDP
Packet size	512 bytes
Nodes number	20, 30, 40, and 50
Connections number	10 in 20 node topology 15 in 30 node topology 20 in 40 node topology 25 in 50 node topology
Transport Buffer Size	20 packets
Number of balck holes	2 in 20 node topology 3 in 30 node topology 4 in 40 node topology 5 in 50 node topology

After each simulation run, a separate trace file is generated that contains all the activities that occurred while running the NS2 simulation. From these trace files, the values of the desired features can be extracted from unwanted large redundant data by using the open source (GAWK) scripting program under Unix operating system, and therefore, these extracted features can be handled comfortably.

V.3. Simulation of Fuzzy Logic System

The fuzzy logic system is built using MATLAB (version 7.12.0) software, because it is convenient and simple when handling the fuzzification and defuzzification methods. Also, due to supporting the Graphical User Interface (GUI) for the fuzzy function. Furthermore, the proposed fuzzification stage is divided into three scenarios, in order to tune fuzzy parameters and reach to the best results. Table III shows each scenario and the features (linguistic variables) with their number of corresponding membership functions in the fuzzy inference system, also shows the number of rules that covers all possibilities. The initial number of rules is reduced because some rules were discarded either for their redundancy or could be combined with other rules.

The Principle Component Analysis (PCA) technique is applied, in order to tackle the delay problem. The PCA is a common technique that employed to reduce space and time complexities of any given system through transforming a huge, highly complex, and multi-dimensional system into a lower-dimensional, less size, and less complex system. The ranges of the variables are determined using analytical information extracted from the trace files produced by NS2 simulator tool, after simulating the given ad-hoc network with and without black hole attack. It is obvious from Table III that the number of membership functions increases while moving from scenario I to scenario II and to scenario III. Consequently, this affects results of simulation for the cross layer IDS as explained later in this section.

TABLE III
SIMULATION SCENARIOS FEATURES, MEMBERSHIP FUNCTIONS, AND FUZZY RULES.

Sc. No.	Feature	Membership Functions No.	Fuzzy Rules No. (Before PCA)	Fuzzy Rules No. (After PCA)
I	*Total Residual Energy*	*3 MFs*	*162 rule (reduced to 70)*	*59 rule*
	Collision	*3 MFs*		
	Dropped Packets	*3 MFs*		
	Buffer Overflow	*2 MFs*		
	Pause Time	*3 MFs*		
II	*Total Residual Energy*	*3 MFs*	*270 rule (reduced to 129)*	*73 rule*
	Collision	*3 MFs*		
	Dropped Packets	*5 MFs*		
	Buffer Overflow	*2 MFs*		
	Pause Time	*3 MFs*		
III	*Total Residual Energy*	*5 MFs*	*1050 rule (reduced to 548)*	*96 rule*
	Collision	*3 MFs*		
	Dropped Packets	*7 MFs*		
	Buffer Overflow	*2 MFs*		
	Pause Time	*5 MFs*		

V.4. Simulation Results

For more reliable testing of our proposed system, performance metrics such as FP, FN, and DR are measured by simulating a large number of randomly generated networks in order to find their averages. Therefore, 1000 different trace files are generated for 1000 different simulation runs for the proposed system. Table IV is a confusion matrix which shows how the metrics of the proposed system are evaluated. Furthermore, table V gives an example on how these metrics evaluated for one of the scenarios for the proposed system, specifically, scenario II with 40 nodes topology.

TABLE IV
CONFUSION MATRIX FOR CALCULATING THE EVALUATION METRICS.

Detected	Actual	
	Black Hole	**Normal**
Black Hole	*Tb*	*Fb*
Normal	*Fc*	*Tc*

TABLE V
SCENARIO II STATISTICS EXAMPLE WITH A TOPOLOGY OF 40 NODES.

Detected	Actual	
	Black Hole	**Normal**
Black Hole	*3784*	*216*
Normal	*54*	*35946*

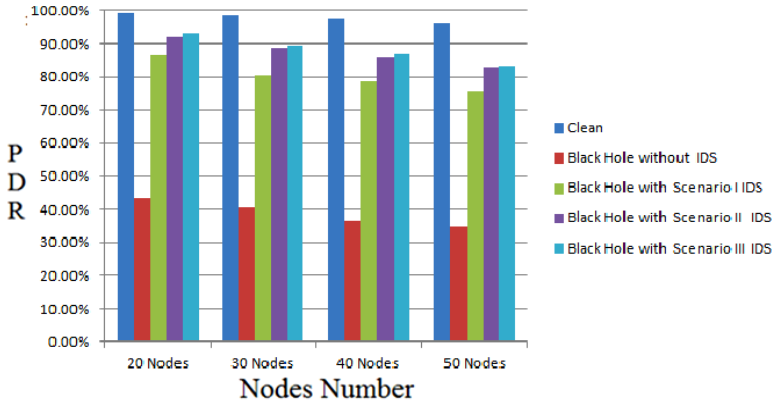

Figure 3: Packets delivery ratio (PDR) with respect to number of nodes for the proposed approach with different scenarios.

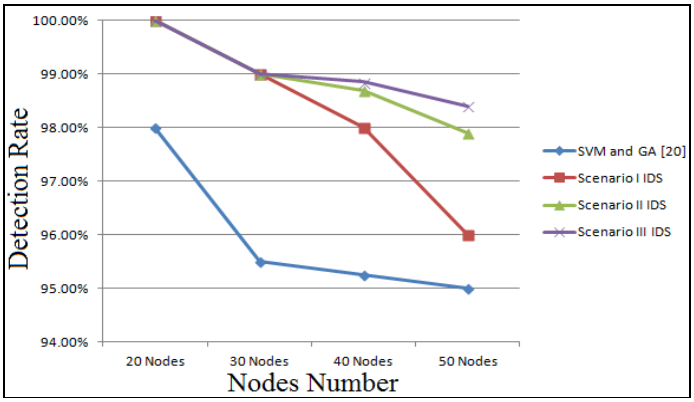

Figure 4: Detection rate with respect to number of nodes for the proposed approach and the studied approach in [33].

Figure 3 shows the resulting PDR at different circumstances as follows: (1) - When network is clean from black hole attacks. (2) - When network is under the black hole attack. (3) - When network is under the black hole attack and the proposed cross layer IDS is implemented with the three scenarios of our proposed approach.

Apparently, figure 3 shows that the black hole has a severe negative impact on the packets delivery ratio, PDR, of network. It is also noticed that after implementing our proposed system for network that is under a black hole attack, there has been a remarkable increase in network's PDR which can reach more than 90% of network that clean from black holes. Furthermore, the PDR values increases when moving from Scenario I to Scenario II, and to Scenario III.

Figure 4 shows the detection rate, DR, for the proposed approach in [33] and our proposed approach scenarios. Clearly, our proposed method outperforms the detection rate of proposed approach in [33], especially in Scenario II and III by a relatively high improvement ratio which can reach up to 4%. The best detection rate belongs to Scenario III; because it fuzzy parameters are mostly tuned in this scenario in order to reach to the best results. However, Scenario I of our proposed approach might have worst detection rate when network's node number is higher than 50 nodes.

Figure 5 shows results false positive rate, FP, with respect to number of nodes, in which comparison between our proposed IDS cross-layer based approach with three scenarios and the cross-layer IDS approach in [33]. Clearly, there is a noticeable improvement regarding the false positive rate when utilizing our cross-layer IDS approach. Our proposed approach-scenario III outperforms the proposed approach in [33] by almost 80% improvement.

The fourth metric that is used to evaluate performance of this work is the false negative rate. A comparison of our proposed system along with other system is shown in Figure 6.

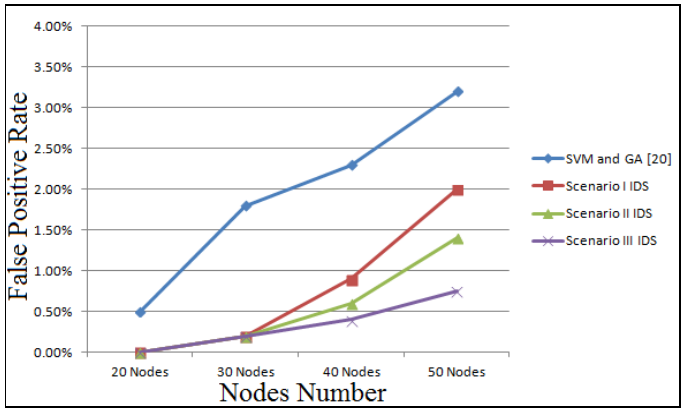

Figure 5: False positive rate with respect to number of nodes for the proposed approach and the studied approach in [33].

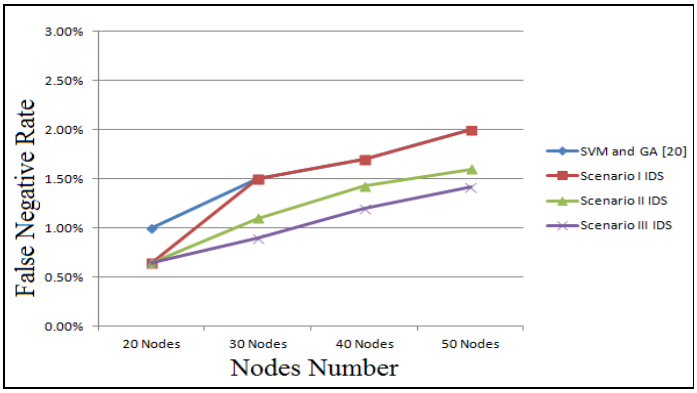

Figure 6: False negative rate with respect to number of nodes for the proposed approach and the studied approach in [33].

Figure 6 shows how our proposed system can achieve a very low false negative rate, FN, which is much better than the proposed system in [33] with almost 50% improvement ratio. Apparently, our proposed approach's enhancement shows up when using Scenario III for different performance metrics.

Finally, the last metric used to evaluate our proposed approach is the end-to-end, E2E, delay which measures

the additional processing time consumed due to implementing our proposed approach in the network. Figure 7 shows the E2E delay of our approach in the three scenarios, and when the network is clean from black holes in order to have a fair comparison and legitimate insights.

Our proposed system has shown impressive results regarding the PDR, DR, FP and FN. However, as seen in Figure 7, an additional minor delay occurs when implementing our approach, especially for scenario III. However, this additional minor delay is acceptable to adopt such system in real life applications and will not dramatically affect the QoS of wireless ad-hoc networks. Furthermore, it is necessary to say that without the use of the PCA technique, the amount of delay will be higher than the acceptable range. Thanks to PCA technique.

VI. Conclusions and Future Work

The nature of wireless ad-hoc networks attracts numerous malicious behaviors such as black hole attack, where at least one dishonest node starts to seduce other honest nodes to use it as the path for their transmitted packets to the desired destination. Conventional counter measures to mitigate such attack mostly depend on a single layer which made them useless in some cases and/or have high false positive rate which results in reducing networks QoS.

We have proposed a novel enhanced cross-layer based intrusion detection system for securing the wireless ad-hoc networks from black hole attacks. The proposed system performs intrusion detection using features extracted from four layers: physical layer, MAC layer, network layer, and transport layer. These extracted features are used as an input for the fuzzy logic system which decides whether a node is a normal node or a black hole node (attacker). This cross-layer IDS is based on the proposed novel fuzzy rules that detect either single or multiple black hole attacks.

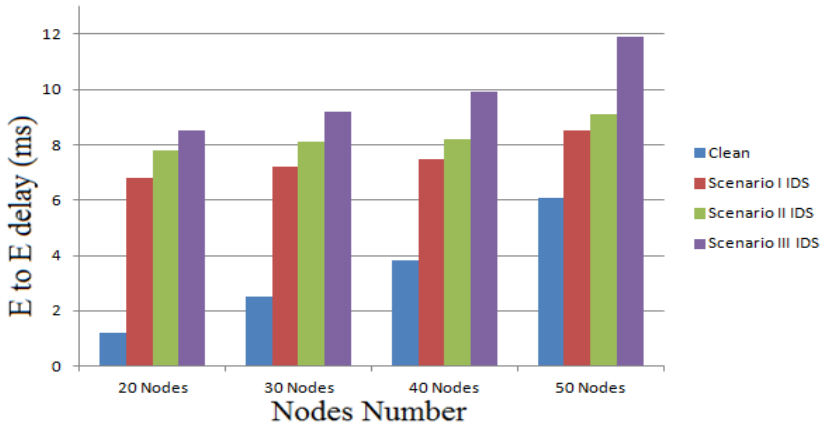

Figure 7: End-to-end (E2E) delay of normal network and the network with IDS, with respect to different number of nodes.

Results have shown that our proposed approach can achieve up to 92% PDR with a remarkable very minor additional end-to-end delay. Moreover, a comparison is made between our proposed approach and other cross-layer approach in literature [33]. Our proposed approach outperforms this existing approach by 80% for false positive rate and by 50% for false negative rate.

As a future work, we plan to make our proposed IDS based fuzzy system able to detect not only single or multiple black hole attacks (as shown in results' section), but also detects the collaborative black hole and grey hole attacks. Specifically, for collaborative black hole attacks, our fuzzy system rules should be tuned or updated to comply with such attacks. Regarding grey hole attacks which has some different characteristics, it may require forcing additional performance metrics and/or increase number of membership functions into our proposed fuzzy system, also it may require tuning current membership functions.

Appendix

Figures 8 and 9 show membership functions' shapes and their ranges for the dropped packets and collision features for scenarios I, respectively. Tables VI and VII illustrate membership functions' ranges for the dropped packets and collision, respectively, for scenario I.

Figure 10 shows the pause time membership functions for scenarios I and II, where their ranges are presented in Table VIII.

Table VI: Dropped packets membership functions and their ranges for scenario I.

Membership Function	Type	Ranges (x,y)
Low	Trapezoid	(-∞,0), (0,1), (0.03,1), (0.17,0)
Medium	Triangle	(0.08,0), (0.5,1), (0.9,0)
High	Trapezoid	(0.7,0), (0.8,1), (1,1), (∞,0)

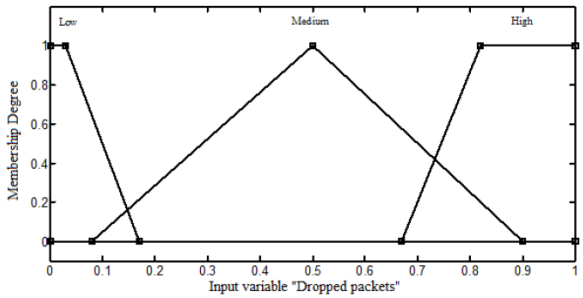

Figure 8: Dropped packets membership functions for scenario I.

Figure 11 illustrates buffer overflow membership functions for scenarios I, II and III, where their corresponding ranges are presented in Table IX. Figure 12 shows the residual energy membership functions for scenarios I and II and their corresponding ranges shown in Table X.

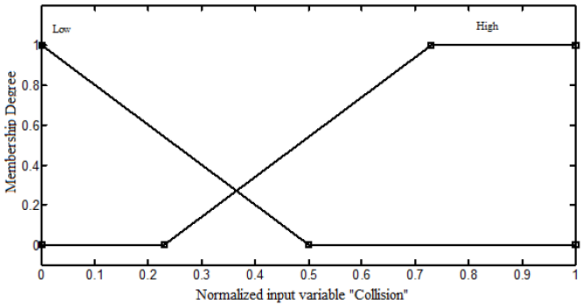

Figure 9: Collision membership function for scenario I.

Table VII: Collision membership functions and their ranges for scenario I.

Membership Function	Type	Ranges (x,y)
Low	Triangle	(-∞,0), (0,1), (0.5,0)
High	Trapezoid	(0.23,0), (0.73,1), (1,1), (∞,0)

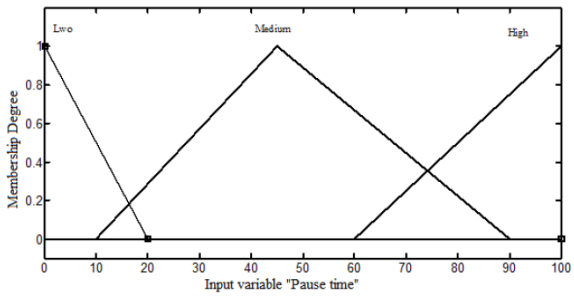

Figure 10: Pause time membership functions for scenarios I and II.

Table VIII: Pause time membership functions and their ranges in scenarios I and II.

Membership Function	Type	Ranges (x,y)
Low	Triangle	(-∞,0), (0,1), (20,0)
Medium	Triangle	(10,0), (45,1), (90,0)
High	Triangle	(60,0), (100,1), (∞,0)

Due to the unnecessary repetition, we have not listed all membership functions' figures and their ranges for the simulated three scenarios. However, scenario II membership functions granularity of ranges is greater than scenario I. Also, scenario III membership functions granularity of ranges is greater than both scenarios I and II, in order to tune fuzzy parameters and achieve better results.

As shown in Figure 13 the residual energy membership functions for scenarios III are illustrated, where their corresponding ranges revealed in Table XI. Clearly, membership functions ranges are tighter over the same ranges, and consequently, results become more accurate and precisely tuned when detecting black hole attacks. For instance, residual energy membership functions for scenario III ranges are: low, slightly low, medium, slightly high, and high. However, in scenario I or II membership function ranges are only: low, medium, and high. That is why scenario III black hole detection accuracy is the best between the three studied scenarios, as shown in results, section V.

Finally, the Black hole membership functions for scenarios I, II, and III are shown in figure 14.

Table IX: Buffer overflow's membership functions and their ranges in scenario I, II and III.

Membership Function	Type	Ranges (x,y)
Under	Triangle	(-∞,0), (0,1), (21,0)
Over	Triangle	(19,0), (20,1), (∞,0)

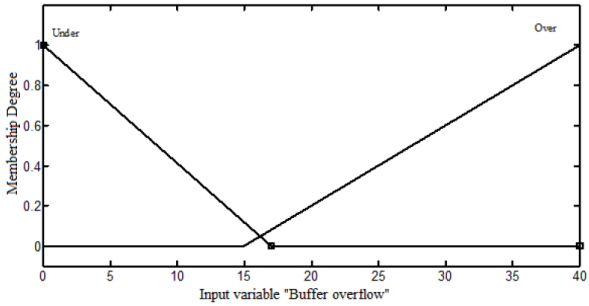

Figure 11: Buffer overflow's membership functions for scenarios I, II and III.

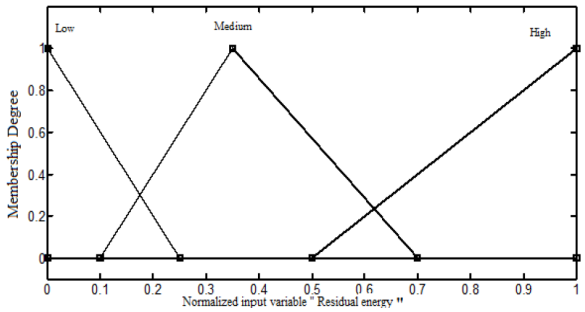

Figure 12: Residual energy membership functions for scenarios I and II.

Table X: Residual energy membership functions and their ranges in scenarios I and II.

Membership Function	Type	Ranges (x,y)
Low	Triangle	(-∞,0), (0,1), (0.25,0)
Medium	Triangle	(0.1,0), (0.35,1), (0.7,0)
High	Triangle	(0.5,0), (1,1), (∞,0)

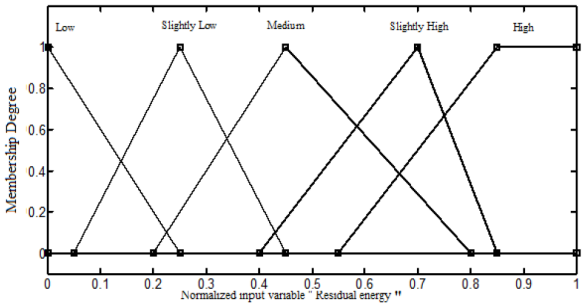

Figure 13: Residual energy membership functions for scenarios III.

Table XI: Residual energy membership functions and their ranges in scenario III.

Membership Function	Type	Ranges (x,y)
Low	Triangle	(-∞,0), (0,1), (0.25,0).
Slightly Low	Triangle	(0.05,0), (0.25,1), (0.45,0).
Medium	Triangle	(0.2,0), (0.45,1), (0.8,0).
Slightly High	Triangle	(0.4,0), (0.7,1), (0.85,0).
High	Trapezoid	(0.54,0), (0.86,1), (100,1), (∞,0)

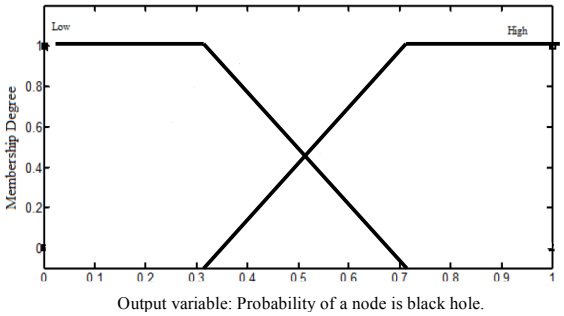

Figure 14: Black hole membership functions for scenarios I, II, III.

References

[1] Khalid A. Darabkh, Wala'a S. Al-Rawashdeh, Raed T. Al-Zubi, and Sharhabeel H. Alnabelsi, "C-DTB-CHR: Centralized Density- and Threshold-based Cluster Head Replacement Protocols for Wireless Sensor Networks," *The Journal of Supercomputing*, , vol. 73, no. 12, pp. 5332-5353, 2017.

[2] Mamoun F. Al-Mistarihi, Rami Mohaisen, Ashraf Sharaqa, Mohammad M. Shurman, and Khalid A. Darabkh, "Performance Evaluation of Multiuser Diversity in Multiuser Two-Hop Cooperative Multi-Relay Wireless Networks using MRC over Rayleigh Fading Channels," *International Journal of Communication Systems*, vol. 28, no. 1, pp. 71-90, January 2015.

[3] Mohammad Shurman, Noor Awad, Mamoun F. Al-Mistarihi, and Khalid A. Darabkh, "LEACH Enhancements for Wireless Sensor Networks Based on Energy Model," *Proceedings of the 2014 IEEE International Multi-Conference on Systems, Signals & Devices, Conference on Communication & Signal Processing,* Castelldefels-Barcelona, Spain, pp. 1-4, February 2014.

[4] Khalid A. Darabkh, Wijdan Y. Albtoush, and Iyad F. Jafar, "Improved Clustering Algorithms for Target Tracking in Wireless Sensor Networks," *Journal of Supercomputing*, vol. 73, no. 5, pp 1952–1977, May 2017.

[5] Ala F. Khalifeh, Mahmoud AlQudah, and Khalid A. Darabkh, "Optimizing the Beacon and SuperFrame Orders in IEEE 802.15.4 for Real-time Notification in Wireless Sensor Networks," *Proceedings of 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET 2017)*, Chennai, India, March 2017.

[6] K. A. Darabkh, B. Abu-Jaradeh, and I. Jafar, "Incorporating Automatic Repeat Request and Thresholds with Variable Complexity Decoding Algorithms over Wireless Networks: Queuing Analysis," *IET Communications*, vol. 5, no. 10, pp. 1377–1393, July 2011.

[7] M. Shurman, M. Al-Mistarihi, and K. Darabkh, "Merging Dynamic Address Autoconfiguration and Security Key Protocols in Mobile Ad Hoc Networks," *Proceedings of 36th IEEE International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2013),* Opatija, Croatia, pp. 441-445, May 2013.

[8] M. Shurman, M. Al-Mistarihi, and K. Darabkh, "Dynamic Distribution of Security Keys and IP Addresses Coalition Protocol for Mobile Ad Hoc Networks," *Automatika – Journal for Control, Measurement, Electronics, Computing and Communications*, In Press.

[9] R. Al-Zubi, M. Krunz, G. Al-Sukkar, M. Hawa, and K. A. Darabkh, "Packet Recycling and Delayed ACK for Improving the Performance of TCP over MANETs," *Wireless Personal Communications*, vol. 75, no. 1, pp. 943-963, March 2014.

[10] Khalid A. Darabkh and Ola Alsukour, "Novel Protocols for Improving the Performance of ODMRP and EODMRP over Mobile Ad hoc Networks," *International Journal of Distributed Sensor Networks*, vol. 2015, pp.1-18, October 2015.

[11] Camp, Tracy, Jeff Boleng, and Vanessa Davies. "A survey of mobility models for ad hoc network research." Wireless communications and mobile computing 2, no. 5 (2002): 483-502.

[12] Alnabelsi, Sharhabeel H., Hisham M. Almasaeid, and Ahmed E. Kamal. "Optimized sink mobility for energy and delay efficient data collection in FWSNs." *IEEE Symposium on Computers and Communications (ISCC),* pp. 550-555, 2010.

[13] Alnabelsi, S.H., and Kamal, A.E. "Interference-based packet recovery for energy saving in Cognitive Radio Networks." *IEEE ICC,* pp. 5978-5982. 2012.

[14] Shurman, M.M.; Al-Mistarihi, M. F.; Alnabelsi, S.H.; Hani, R.R. "A Novel Network Coding Approach: Packets Conflict Based For Matrix Optimization." *Journal of Theoretical & Applied Information Technology* 95, no. 20 (2017).

[15] Dokurer, Semih, "Simulation of Black hole attack in wireless Ad-hoc networks". Master's thesis, Atılım University, Sept. 2006.

[16] K. S. Madhusudhananaga Kumar and G. Aghila, "A Survey on Black Hole Attacks on AODV Protocol in MANET," *International Journal of Computer Applications*, Oct. 2011.

[17] Y. Hu, A Perrig, and D. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks," *Proc. of IEEE INFORCOM*, Nov. 2002.

[18] F. Xing and W. Y. Wang, "Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks," *MILCOM*, Washington DC, Oct. 2006.

[19] S. Sharma and R. Gupta, "Simulation study of black hole attack in the mobile ad-hoc networks," *Journal of Engineering Science and Technology*, Dec. 2009

[20] H. Yadav, R. Kuma, "Identification and Removal of Black Hole Attack for Secure Communication in MANETS," *International Journal of Computer Science and Telecommunications*, 2012.

[21] B.Kannhavong, H.Nakayama, Y.Nemoto, N.Kato, A.Jamalipour, "A Survey Of Routing Attacks In Mobile Ad Hoc Networks," *IEEE Wireless Communications*, Oct. 2007.

[22] Kanthe, A., Simunic, D., and Prasad, R., "Comparison of AODV and DSR On-Demand Routing Protocols in Mobile Ad hoc

Networks," *1st International Conference on Emerging Technology Trends in Electronics, Communication and Networking (ET2ECN)*, Dec. 2012.
[23] Mohammad Al-Shurman, Seong-Moo Yoo, and Seungjin Park, "Black hole attack in mobile Ad Hoc networks," *in Proc. of the 42nd annual Southeast regional conference, ACM Southeast Regional Conference*, Huntsville, April 2004.
[24] Banerjee, Subhashis, Mousumi Sardar, and Koushik Majumder. "AODV Based Black-Hole Attack Mitigation in MANET," *Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013*. Springer International Publishing, Switzerland, June 2014.
[25] Jaisankar N, Saravanan R, Swamy KD, "A Novel Security Approach for Detecting Black Hole Attack in MANET," *the International Conference on Recent Trends in Business Administration and Information Processing*, India, March 2010.
[26] Latha Tamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET," *J. of Networks*, 2008.
[27] Medadian, M., Mebadi A., Shahri E., "Combat with Black Hole attack in AODV routing protocol," *IEEE 9th Malaysia International Conference on Communications (MICC)*, 2009.
[28] Tamilselvan L, Sankaranarayanan V., "Prevention of Black hole Attack in MANET," *the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, Australia, August 2007.
[29] J Alem, Y.F., Zhao Cheng Xuan , "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," *2nd International Conference on Future Computer and Communication (ICFCC)*,China , May 2010.
[30] J Lin, Wei, Liu Xiang, Derek Pao, and Bin Liu. "Collaborative distributed intrusion detection system," *Second International Conference on Future Generation Communication and Networking, (FGCN08)*, China, July 2008.
[31] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda," Detecting Black and Gray hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method ", *international journal of emerging technology and advanced engineering*, Jan. 2012.
[32] Babu, K. Suresh, and K. Chandra Sekharaiah, "CLDASR: Cross Layer Based Detection and Authentication in Secure Routing in MANET," International Journal of Computer Networks and Wireless Communications, April 2014.
[33] T. Poongothai, K. Duraiswamy "Cross Layer Intrusion Detection System of Mobile Ad Hoc Networks using Feature Selection Approach," *WSEAS Transactions on Communications*, 2014.
[34] A. Mohammed, B.H. Sofiane and F.K. Mohamed "A Cross Layer for Detection and Ignoring Black Hole Attack in Manet" *I.J. Computer Netw. & Information Security*, 10, pp. 42-49, 2015.
[35] Baiad, Raghad, Omar Alhussein, Hadi Otrok, and Sami Muhaidat. "Novel cross layer detection schemes to detect blackhole attack against QoS-OLSR protocol in VANET." *Vehicular Communications 5* (2016): 9-17.
[36] Gopal, Usha, and Kannimuthu Subramanian. "A secure cross-layer AODV routing method to detect and isolate (SCLARDI) black hole attacks for MANET." *Turkish Journal of Electrical Engineering & Computer Sciences 25*, no. 4 (2017): 2761-2769.
[37] Subba, Basant, Santosh Biswas, and Sushanta Karmakar. "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation." *Engineering Science and Technology, an International Journal 19*, no. 2 (2016): 782-799.
[38] Wahane, Gayatri, Ashok M. Kanthe, and Dina Simunic. "Technique for detection of cooperative black hole attack using true-link in Mobile Ad-hoc Networks." *In IEEE 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1428-1434, 2014.
[39] Feizollah, Ali, Nor Badrul Anuar, Rosli Salleh, and Ainuddin Wahid Abdul Wahab. "A review on feature selection in mobile malware detection." *Digital Investigation 13* (2015): 22-37.
[40] Patel, Nirav J., and Rutvij H. Jhaveri. "Detecting packet dropping nodes using machine learning techniques in Mobile ad-hoc network: A survey." *In IEEE International Conference on Signal Processing and Communication Engineering Systems (SPACES)*, pp. 468 - 472, 2015.
[41] Kaur, Ramanpreet, and Anantdeep Kaur. "Blackhole Detection in MANETs Using Artificial Neural Networks." *International Journal for Technological Research in Engineering 1*, no. 9 (2014): 959-962.
[42] Abdulkader, Zaid A., Azizol Abdullah, Mohd Taufik Abdullah, and Zuriati Ahmad Zukarnain. "LI-AODV: Lifetime Improving AODV Routing for Detecting and Removing Black-Hole Attack from VANET." *Journal of Theoretical and Applied Information Technology 95*, no. 1 (2017): 196.
[43] Q. Shen, R. Jensen, "Rough sets, their extensions and applications," *International Journal of Automation and Computing*, May 2007.
[44] C. Tsai, W. Eberle, C. Chu, "Genetic algorithms in feature and instance selection," *in Knowledge-Based Systems*, vol. 39, 2013.
[45] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda, "Detecting Black and Gray hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method," *International Journal of Emerging Technology and Advanced Engineering*, Jan. 2012.

Author's information

[1,2,3]Jordan University of Science and Technology, Jordan.
[4]Al-Balqa Applied University, Jordan.

Dr. Mohammad M. Shurman received the B.Sc. degree in Electrical and Computer Engineering from Jordan University of Science and Technology, Jordan, M.Sc. and Ph.D. degrees in Computer Eng.-Wireless Networks from University of Alabama-Huntsville (UAH) in 2000, 2003, and 2006, respectively. Presently, he is an associate professor in Network Eng. and Security Dept., JUST, Jordan. His research interests include wireless ad-hoc networks, security, WSNs, network coding, mobile networks, SDN, cognitive radio, 4G and 5G technologies.

Prof. Omar M. Al-Jarrah received the B.Sc. in Electrical Engineering from JUST in 1991, M.Sc. and Ph.D. in Electrical and Computer Engineering from Ohio State University in 1994 and 1996, respectively. He is serving as a university president and a professor of computer engineering, Jordan University of Science and Technology. Professor Omar research interests are intelligent systems, robotics, and computer networks areas, web computing, and e-learning. Previous research areas include Multiprocessor Systems and Intelligent Control.

Salem Esoh got his B.Sc. in communication and software engineering, Al-Balqa Applied University, Jordan, 2011, and his M.Sc. in computer engineering, JUST, Jordan, 2015. His research interests focus on developing IDS for wireless networks. Currently, he is an engineer at Mitsubishi Elevators and Escalators, Jordan.

Dr. Sharhabeel H. Alnabelsi is an assistant professor at Computer Engineering Dept. at Al-Balqa Applied University, Amman, Jordan. He received his Ph.D. in computer engineering from Iowa State University, USA, 2012. Also, he received his M.Sc. in computer engineering from The University of Alabama in Huntsville, USA, 2007. Dr. Alnabelsi research interests include cognitive radio networks, wireless sensors networks, and network optimization.

