IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 28, 2020, accepted January 11, 2021, date of publication January 13, 2021, date of current version January 22, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3051491

A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET)

MUHANNAD TAHBOUSH[1] **AND MARY AGOYI**[2]
[1]Department of Computer Engineering, Cyprus International University, 10 Mersin, Turkey
[2]Information Technology Department, School of Applied Sciences, Cyprus International University, 99258 Nicosia, Turkey

Corresponding author: Muhannad Tahboush (mh_tahboush@yahoo.com)

ABSTRACT Mobile Ad-hoc Networks (MANET) are decentralized wireless networks that communicate without pre-existing infrastructure. MANETs are vulnerable to the most popular types of attacks and threats, such as wormhole attacks. A wormhole attacks is very challenging issues that records the packets from one location of the network and tunnels them to another location to undermines the performance of the wireless network and disrupt the most routing protocol. However, the existing solutions have been developed to overcome the wormhole attack, but still suffering from additional hardware, incur high delay delivery, or fail to provide high throughput, packet delivery ratio as well as consume higher energy. In this paper a hybrid wormhole attack detection (HWAD) algorithm is proposed, which is able to detect both in-band wormholes through performs round trip time (RTT) based on its hop count, and packet delivery ratio (PDR), also out-of-band wormholes through performs transmission range between successive nodes in a more optimistic manner than existing solutions. HWAD reduce the delay and energy through avoids performing wormhole detections for all available nodes in the network. HWAD does not rely on any special hardware and middleware. The proposed algorithm HWAD was executed using NS-2 network simulator. The performance metrics was taking into consideration to evaluate the performance of the proposed algorithm the throughput, end to end delay, packet delivery ratio, and consuming energy. The proposed algorithm utilized Ad-hoc On-Demand Distance Vector (AODV) routing protocol to improve the detection method. The experimental results have shown the performance metrics of the proposed approach HWAD outperformed in wormhole detection compared with other algorithms.

INDEX TERMS Wormhole attack, malicious node, legitimate node, AODV, MANET.

I. INTRODUCTION

With rapid development and increases in the volume of wireless mobile computing technology that has driven a revolution within the computing world, ad-hoc networks have emerged in many forms. Mobile Ad-Hoc networks is a collection of wireless mobile node which communicate directly with each other within its radio coverage to form a temporary networks without pre-existing infrastructure or central base stations [1], [2]. MANET is an unreliable, open medium, self-configured wireless networks and the process of dynamic device communication where the participating node can enter or leave is simplified. This leads to changing network topology rapidly and unpredictably [3]. Routing protocols play an important role in wireless network to route the packet over multiple hops and from one node to another, it is the backbone of wireless networks and have ability to show the shortest path from source and destination to achieve specific tasks [4]. In addition, some routing protocols specialized for using in wireless networks with low power consumption [5].

In MANET, the participating node has a limited transmission range. Therefore, two nodes will not be able to communicate With each other if they are not in the range of radio coverage of each other. Thus, the transmission through multi-hops scenario will be employed and the intermediate node has to forward the packet to the next node until it reaches the destination [6]. Due to the wireless transmission spontaneous nature and characteristics of MANET, this makes MANET prone to several type of attack and security threats such as wormhole attack [7], [8]. Thus, it's important to ensure the confidentiality of data transmission in the wireless network from node to node without compromising data transmission integrity.

The wormhole attacks is very challenging issues and one of the serious security threats in detection to MANET. The wormhole attack initiated when an adversary create a

The associate editor coordinating the review of this manuscript and approving it for publication was Dongxiao Yu.

communication link between two distant nodes by captures the packet from one location of the network and sends it to unauthorized location of the network. To generate fake connections, mislead the legitimate path, changing or dropping the sent packets which will lead in giving a false network topology [7], [9] and [10] as shown in Fig.1. The attackers are directly connected with each other. Thus, it has the ability to connect faster than legitimate nodes to carry out the attack.

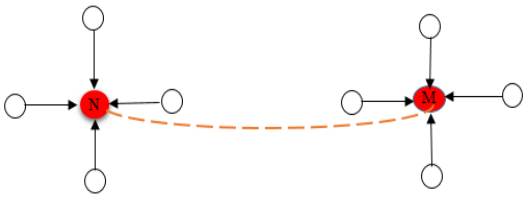

FIGURE 1. Communication link connecting N and M wormhole nodes.

However, the tunnel can be formed through Packet encapsulation (in-band) that is forwarding the packet through available legitimate nodes in the network. The out-of-band channel which is also forwarding packets over long distances and use separate external communication link between malicious nodes [11]. In out-of-band attack, the source node and destination node are away from each other. But, due to the fake created tunnel they appear that they are near and direct neighbours of each other which will reduce the hop count. On the other hand, in-band attack use legitimate routes and actual hop count does not increases during traversal.

A wormhole attack does not require the knowledge of a security system, which includes cryptography mechanisms, public/private keys, etc. Thus cannot be detected using cryptographic mechanisms, therefore, even if the transferred packet was encrypted with any type of encryption, the malicious node will be able to tunnel the packet to another distant malicious node [12] and [13].

There are some challenges that are required to be solved through the proposed approach HWAD. These challenges are the network incur high delay delivery, fail to provide high throughput, packet delivery ratio as well as consume higher energy. Therefore, this study proposes an algorithm that relies on three detection mechanisms of wormhole attack that is based on the AODV protocol. The proposed algorithm combines RTT based on its hop count, PDR and transmission range features to obtain high accuracy of wormhole attack detection. The proposed algorithm was implemented for both out-of-band and in-band wormhole attack and the K-Means clustering algorithm has been employed in this study to determine threshold value in packet delivery ratio, it is a widely used algorithm in the field of data mining. Additionally, K-means is an iterative and powerful algorithm which loops until it converges to a locally optimized solution [14]. Thus, we propose the HWAD and the contributions of this paper are summarized as follows:

1- We proposed a novel HWAD secure algorithm for wormhole detection in MANET. HWAD is able to detect both in-band wormholes and out-of-band wormholes through perform transmission range between successive nodes, round trip time based on its hop count, and packet delivery ratio to detect the existence of wormhole.
2- The concept of (NRT) threshold, will avoids launch wormhole detection for all nodes in MANET, resulting in improving the performance and accuracy of wormhole detection and saving energy as well as reduce the delay.
3- We formally employed the K-Means clustering algorithm to find out the best optimal centroid value that will be used as packet delivery ratio threshold in in-band detection.
4- We test the performance of HWAD by simulating and comparing it with two other well-known wormhole detection algorithms, Aliady and Al-Ahmadi [48] and MCRP [47]. The results demonstrate that our approach outperforms existing approaches.

The remaining of this paper is organized as follows. Section I provides the introduction. Section II literature review. Section III technical preliminaries. Section IV shows the proposed algorithm. Section V describe security analysis. Section VI provides simulation setup and parameters. Section VII shows result comparison and evaluation. Finally section VIII, the conclusion

II. LITERATURE REVIEW

Several algorithms and scientific studies that have been devoted for MANET. Some of these algorithm require specialized hardware or incur high communication overhead. However, we will concentrate on literature on some of the prevailing solutions on MANET and give brief description of all the relevant literature reviewed.

Chiu and Lui [15] Propose wormhole detection method called delay per hop indication (DELPHI). DELPHI perform multipath approach and calculates mean delay per hop of every path. The sender calculate mean delay per hop of each route. Thus, wormhole nodes can be detected if the path that has longer delays and will not be selected to transmit the data packet. Due to the information and detection that DELPHI perform at the sender, it does not require synchronized clock to determine the positioning of the node.

Amish and Vaghela [16] Propose an extension to AODV to detect wormhole attack called Ad-hoc On-demand Multipath Distance Vector routing protocol (AOMDV). the proposed method based on RTT calculation from the source to destination for every route, then, it divide the value of RTT by corresponding hop count and the average value is a threshold value and compare the RTT value with the threshold to determine the existence of wormhole.

Tun and Maw [17] Proposed a wormhole detection mechanism based on RTT and neighbour number. The consideration in here is that the adversary can increases the number of

neighbours of the nodes within the radius, to provide inaccurate RTT value between successive nodes. Therefore, when the RTT value between two successive nodes is high and the neighbour number is considerable greater than the average neighbour number, there is a suspect that a wormhole path is in between.

Capkun *et al.* [18] propose a method called secure tracking of node encounters (SECTOR) against wormhole attack. The distance between two nodes can be calculated based on the speed of data transmitted. The detection method measure the time between sending out a challenges bit and receiving the response, the first node will compute an upper bound of the distance which is between these two nodes, after than, check whether this distance violates and physical constraints.

Lai [19] Propose a method against wormhole attack, by applying the standard routing protocol IPv6 for Low Power and Lossy Networks (RPL). However, this approach delimits the maximum distance that a packet can take in the transmission. The rank of a node defined RPL is adopted to measure the distance. The proposed detection method discovers malicious wormhole nodes if unreasonable rank values are identified.

Hu *et al.* [20] propose wormhole attack detection mechanism based on packet leashes. The proposed methodology consider both geographical and temporal leashes. The geographical rely on current location and transmission time associate with the packet. The receiving node will compute the distance to the sender and the time it took the packet to traverse the path to determine whether the packets recipient within a certain distance from the sender. In temporal leashes, based on clock that is tightly synchronized but do not rely on GPS information. The sending node will associate the transmission time and the expiration time to every sent packet to restrict the packet to travel over long distances, and at the receiving node will use its own packet reception time for verification. By using compute lightweight operations which will determine whether the packet pass through the wormhole path.

Hu and Evans [21] Proposed mechanism based on directional antennas to prevent wormhole attacks. Neighbour lists will be built in a secure way by using the direction in which a signal is heard from a neighbour with the assumption that the antennas on all the nodes are aligned. However, it only prevents the kind of wormhole attacks in which malicious nodes try to deceive two nodes into believing that they are neighbours.

Chen *et al.* [22], propose a distance-consistency-based secure localization scheme that is employed against wormhole attack. It consist of three different phases of detection of wormhole attack. Firstly, detect and identifies whether it is under a duplex wormhole attack or a simplex wormhole attack. And second, the valid locator's identification, different identification schemes are proposed to identity the V-locators. Third, self-localization, after identifying the V-locators, the sensor conducts the self-localization using the MLE method with correct distance measurements.

Jamali and Fotohi [23] Proposed a method against wormhole attack through Artificial Immune System (AIS) which is able to protect against a set of extraneous attacks without affecting the overall performance of the network. The proposed approach consist of two phases, in the first phase a test packet will be employed and sent from each route and the destination is obliged, a confirmation packet will be send upon receiving test packet. Thus, if the route contain wormhole nodes, the packet will not reach its destination and validation packet will not be received. While in the second phase, usually wormhole attack having lower hop count compare with actual nodes. Thus, when having a low number of hop counts in a route, the possibility of pollution of this route would increase. Which is the situation with a low round trip time and an increase of total energy of the existing nodes in the route.

Tamilarasi and Santhi [24] Proposed a method against wormhole attack in MANET through identifying the wormhole and select the best path. Initially, several path will be generated between source and destination called 'K' using Ad-hoc on demand Multipath Distance Vector (AOMDV) routing protocol. Then, the wormhole attacked path will be identifies through source node by verifying the Detection Packet (DP) and Feedback Packet (FP) from the destination. After determine the wormhole attacked paths, the source node will selects the best path among the attacker free paths using Particle Swarm Optimization (PSO) algorithm and forwards the data to the destination through the best path.

Sankara and Murugaboopathi [25] Proposed mechanism based on Quality of Service (QoS) for entire network to detect the wormhole attacks. The modified secure AODV protocol (MSADOV) has been proposed which uses the packet forward ratio and round trip time to prevent the wormhole attack in MANET. In addition, the proposed approach able to detect both active and passive attacks.

Jamali and Fotohi [26] Proposed a method against wormhole attack called defending against wormhole attack (DAWA) that employ employs fuzzy logic system and artificial immune system. First phase will select high performance route between the source and the destination using fuzzy logic approach. While the second phase will use artificial immune system (AIS) based defines scheme against wormhole attack, where antibodies are trained to detect and eliminate malicious antigens.

Aswale and Joshi [27] proposed wormhole attack prevention using hybrid cryptography algorithm. The proposed technique uses Modified Rivest, Shamir, Adleman (MRSA) and AES for secure and energy-efficient data transmission from source to destination over public channels. Because AES encryption more efficient for large amount of data and does not require high energy, so, it will be used for plaintext encryption and RSA use to encrypt AES key. Thus, AES will encrypt the data of source node.

Fotohi *et al.* [28] proposed wormhole attack detection system using agent-based self-protective method for unmanned aerial vehicle networks (ASP-UAVN). The source node will

initiate route request (RREQ) to the destination to detect the existing routes. Then, once the route reply (RREP) is received, a self-protective method using agents and the knowledge base is employed to choose the safest route among other routes and detect the attacking UAVs. This mechanism will protect the network against wormhole, selective forwarding and sink hole attacks.

III. TECHNICAL PRELIMINARIES

In this section, we characterize the preliminaries that required to achieve this study.

A. ADVERSARY MODEL

The network is established in an antagonistic environment where the adversaries are present. We assume that the adversaries are able to eavesdrop, record and replay messages, including routing protocol messages. Furthermore, the adversary can compromise the legitimate nodes, allowing them to extract their cryptographic secrets messages. This give the opportunity for the adversary to deploy and control a malicious node. The adversary capable of colluding with other malicious nodes. One of these collusion attack is the wormhole.

B. WORMHOLE ATTACK DESCRIPTION

A wormhole attack is one of the gravest attacks that are considered a challenging problem and can be launched at the network layer of the OSI model [29]. It consists of two malicious nodes involved in the routing path and communication link between them as illustrated in Fig.1 between N and M wormhole nodes. The attacker receives packets at one location in the network and send them to a remote location in the network and then replays them locally. The tunnel can be created in many ways such as in-band and out-of-band. The routing path between source and destination will be selected through the created tunnel [9], [30], [31] and [32], which will be used later for packets exchange between malicious nodes. Because of unauthorized access by malicious nodes, the packet can be dropped and cause delay in time for important packet to reduce the network performance or send to another network and at end the network will be disrupted.

Wormhole attack can be classified into four modes of attack operations, which are, packet encapsulation, high power transmission, packet relay and out-of-band. The tunnel can be launched through wired and wireless transmission or an optical link as mentioned in [33], [35]. The packet will be forwarded through distant wormhole nodes by creating an illusion that they are close to each other whereas in reality, they are not. Malicious nodes are equipped with higher transmission power and higher bandwidth in comparison to other legitimate nodes. Therefore, they can transmit packets over long distances to create fake shortcuts, preventing the legitimate nodes to be discovered by its neighbours, creating incorrect routing paths, and then causing network disruptions [34], [35] and [36]. This fake shortcut path which is created by wormhole node will be employed for packet exchange among themselves.

1) IN-BAND WORMHOLE ATTACK

Based on the medium used, the packets can be tunnelled through an in-band and out-of-band attack between two distant malicious nodes [37]. In in-band attacks, the assailants will use the legitimate nodes that have been compromised and the valid existing wireless medium for building a link between malicious nodes. Which will perform the attack on any unprotected packets while packet transmission as illustrated in Fig.2. Assume that the source node denoted S and destination node denoted D, in that case the routing path is S, M1, A, B, M2, D forms an in-band attack. Therefore, In-band attack is very dangerous and does not need extra hardware to launch it [38], [39] and [40]. In addition, unlike out-of-band attack, in-band attack will consume the normal nodes energy due to the usage of these nodes to perform the attack and route the packet over long path.

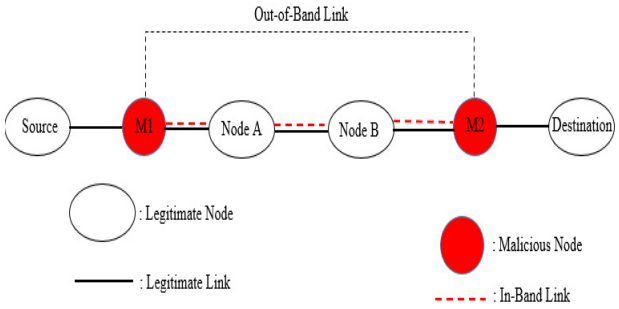

FIGURE 2. Wormhole attack construction between M1 and M2.

2) OUT-OF-BAND WORMHOLE ATTACK

Whereas an out-of-band attack that initiated through different wireless medium via a side channel. Such a channel has high-gain directional antennas, between two distant nodes to prevent legitimate node from appearing. Creating an illusion to the source a link that has fewest number of hops and the destination is near but in reality they are not. As illustrated in Fig.2, the routing path is S, M1, M2, and D to form an out-of-band attack. Therefore, it requires high transmission mode and long range wireless transmission compared to legitimate node [38], [39] and [40] that will enable the wormhole node to construct a direct tunnel between pairs of malicious nodes located away from one another. Thus, the network performance will be disrupted and packets dropped, once the adversary take control over a large amount of packets that passing through the wormhole tunnel.

C. OVERVIEW OF AODV PROTOCOL

To gain appropriate route toward the destination. Routing protocols fall in the place, which are the backbone of the wireless network. Various routing protocols have been

proposed for MANET such as proactive and reactive routing protocols. One of the popular reactive routing protocol as well as intended for use in wireless and mobile ad hoc networks is Ad-hoc On-demand Distance Vector (AODV) [41]. AODV uses less bandwidth, routing overhead and fast convergence while transmission. AODV supports both unicast and broadcast routing, which used when the source node routing table does not contain valid route to the destination to determine the path for communication. Therefore the source will generate on demand route discovery processes and transmit a packet to the preferred destination through intermediate nodes. AODV employ four different types of messages, Route Request (REQ), Route Reply (RREP), Route Error (RERR) and hello (HELLO) message to find and maintain the path to the destination [41], [42]. Route discovery process in AODV protocols illustrated in Fig.3 that show route request RREQ and route reply RREP operations in Fig.4.

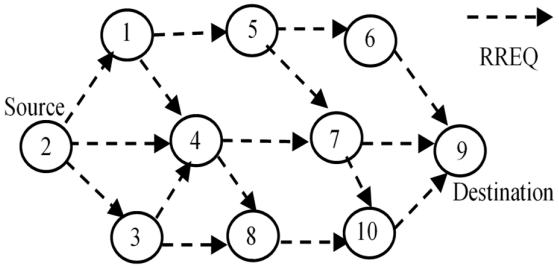

FIGURE 3. Route request RREQ operation.

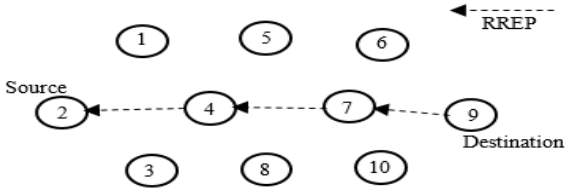

FIGURE 4. Route reply RREP operation.

When the source is willing to send packet to destination, it broadcasts route request (RREQ) during route discovery process. As show in Fig.3, assume the source (node 2) need to communicate with the destination (node 9). If the source node has no valid route to the destination, the broadcasted packets will be forwarded and the process of RREQ will be repeated through intermediate nodes with the least hop count till RREQ message reach the appropriate destination.

Whenever the destination receives the RREQ packet through intermediate nodes with recent information about the shortest route, it will reply with route reply (RREP) message to the source as illustrated in the Fig.4. Where the destination (node 9) will reply with unicast routing, which is a reverse route through the intermediate nodes that are node 7 and node 4, till the packets reach the original source (node 2) and then the exchanging of data packets will be started among them. AODV is very popular routing protocol and designed to be self-starting in an environment of mobile nodes.

D. K-MEANS CLUSTERING ALGORITHM

K-Means is an unsupervised clustering algorithm and best suited for data mining and computationally faster than the hierarchical clustering even for really big data sets and easy to implement [43], [44]. The K-means is a popular technique for intrusion detection and able to detect suspicious and abnormal network user behaviour in a network traffic. The algorithm use the distance as a metric and the given K classes in the data set. After that, the algorithm calculates the average distance providing the initial centroid along with each class described by the centroid as illustrated in (1). The objective of K-Means is to find the best optimal centroid value that will be used as PDR threshold. The algorithms mathematically represented as indicated in the [45].

$$\mathrm{d} = \sum_{k=1}^{k} \sum_{i=1}^{n} \| (x_i - u_k) \|^2 \tag{1}$$

Here, d represent the distance, k represents K cluster centre, u_k represents the kth centre and finally x_i represents the ith point in the data set.

Now, to find out the centroid we derive the equation (1).

$$\begin{aligned} \frac{\partial}{\partial u_k} &= \frac{\partial}{\partial u_k} \sum_{k=1}^{k} \sum_{i=1}^{n} (x_i - u_k)^2 \\ &= \sum_{k=1}^{k} \sum_{i=1}^{n} \frac{\partial}{\partial u_k} (x_i - u_k)^2 \\ &= \sum_{i=1}^{n} 2(x_i - u_k) \end{aligned} \tag{2}$$

If we assume (2) equal to 0. The centroid value can be calculated by using (3).

$$u_k = \frac{1}{n} \sum_{i=1}^{n} xi \tag{3}$$

Therefore, the proposed detection algorithm employs the K- Means in packet delivery ratio as illustrated in the following procedures.

1. Randomly selects K of the objects from 0-1 as initial value for K-Means algorithm, where each object initially represents a cluster mean or centroid. The remaining objects will be similar, assigns each object to the cluster.
2. The trace file (which store coverage information and overall network information) values that resulted from the NS-2 will be used as input value for clustering.
3. Then, computes the new mean or centroid for each cluster, and iterate to find the best performance cluster for different initial values 0-1.
4. Finally, calculate the new mean (centroid) value for the best selected cluster and this centroid will be considered as input for the simulator (use as PDR threshold).

IV. PROPOSED HYBRID WORMHOLE ATTACK DETECTION ALGORITHM

The proposed algorithm is based on Hybrid Wormhole Attack Detection (HWAD) in mobile ad-hoc network. It has been

introduced a neighbour ratio threshold (NRT) to avert performing wormhole checking in all available nodes. Then, the detection algorithm will be employed to combine various detection methods. The proposed algorithm procedures are.

Step 1: Employ a technique called neighbour ratio threshold (NRT) to minimize the number of nodes needed to be detected, as shown in the algorithm 1.

Step 2: After that, determine whether the neighbouring nodes lay in the transmission range of the source or not. If it is outside range of the source, then classify it as out-of-band wormhole attack, as shown in the algorithm 2. Otherwise move to step 3.

Step 3: Finally, employ round trip time based on its hop count and packet delivery ratio to determine the in-band attack in case of the neighbouring nodes are in the transmission range of the source as shown in algorithm 4.

Algorithm 1 Neighbor Ratio Threshold (NRT).

Start

for*each node* n_i *in* N *and its neighbor set* S_i *in* S **do**
  Let $s_i = |S_i|$ (which is the neighbor number of n_i);
  for*each node* $n_j \epsilon S_i$ **do**
    $s_j = |S_j|$ (which is the neighbor number of n_j);
    Set $a = 0$;
      $a = a + s_j$;
  To find the average neighbor number of n_i's neighbors, Then $\bar{si} = \frac{a}{si}$
  To Find the n_i's neighbor ratio $NRT_i = \frac{si}{\bar{si}}$
  if*$NRT_i > NRT$* **then**
    put *ni* to suspected nodes set *A area*;
  end

End of Pseudocode.

A. ASSUMPTIONS

In this section, some assumptions are presented regarding network and opponent capabilities in the proposed design in MANET.

- Assumption 1: It was assumed that, two nodes are considered neighbours if the distance between them is within the transmission range.
- Assumption 2: In the proposed model, the nodes start with the same energy level and have a random speed and mobility direction.
- Assumption 3: The malicious nodes can launch many kinds of wormhole attacks.
- Assumption 4: All mobile nodes are randomly distributed in 2-dementional square network.

B. NEIGHBOUR RATIO THRESHOLD (NRT)

One of the most energy consuming methods as well as increasing delay for nodes in the network is the process of checking whether every single node was affected by a wormhole or not. Generally, the wormhole does not attack all the nodes in a wireless network. Wormhole increases the number of neighbour nodes which causes inaccurate RTT and increases the connectivity of the network. Therefore, a simple effective technique has been used that is called Neighbour Ratio Threshold (NRT). It will compare the neighbour number of a node with all its neighbours to avoid launching the wormhole detection on all nodes in MANET.

After neighbour discovery processes, the nodes will know their neighbours. Then, the node calculates the ratio of its neighbour number and the average neighbour number ($\bar{si}$) of all its neighbours, named the neighbour ratio. Then, the neighbour ratio (*NRTi*) will be compared with the Neighbour Ratio Threshold (NRT) to determine whether wormhole detection is needed or not as illustrated below in algorithm 1, where the entire network E contain nodes N and their neighbours set S.

After that, the nodes which have neighbour ratio higher than neighbour ratio threshold (NRT) will be added to the suspected list to perform out-of-band attack detection as shown in (Algorithm 4) and in-band attack detection as shown in (Algorithm 7). Reducing the delay and energy consumption are main goals for (NRT) whereas performing detection methods.

C. OUT-OF-BAND WORMHOLE DETECTION

1) TRANSMISSION RANGE PHASE

To illustrate this phase of the proposed algorithm, it's important to identify the nodes within its communication range for each network nodes. This phase relies on the transmission time between every two successive nodes to conclude the transmission range of every node. The nodes that are not in range of the source node will be considered as malicious nodes, due to limited radio coverage and the distribution of the legitimate nodes which are closer to one another. Thus, if the link between the nodes has a high transmission time, it would be classified as an out-of-band wormhole. Transmission time between nodes are proposed and calculated to find out the out-of-band attack using hello intervals between Hello Packets, as shown below.

Hello Interval = 2nd Hello_Packet – 1st Hello_Packet

Lemma 1: let T_1, T_2 are two period of time respectively such that $T_1 < T_2$. Then the difference between T_2, T_1 equal T_2 - T_1.

Proof: Let

$$\begin{aligned} T_1 &= T_0 \\ T2 &= T0 + \Delta \\ T2 &= T1 + \Delta \\ \Delta &= T2 - -T1 \end{aligned}$$

Thus, mathematically it is defined as.

$$\text{Transmission Time(TT)} = T_2 - T_1 \tag{4}$$

From the equation (4) we can find out the length of time that needed for packet to travel between nodes to know the range of the node that determined by calculating the Hello Interval. The objective of this phase is to detect whether there

are out-of-band wormhole nodes in the path. As illustrated in the algorithm 2.

Algorithm 2 Out-of-Band Detection Algorithm

Input:Transmission Time (TT) value, threshold value.
Output: out-of-band detected.

1. Star
2. Nodes are deployed using AODV protocol
3. Calculate the transmission time for each node in the routing table.
   TT= Hello Packet 2 - Hello Packet
4. If (TT < threshold) then
5. Neighboring node in the range of source node
6. No Out-of-band wormhole detected, go to algorithm 4
7. else
8. Out of band detecte
9. End of Pseudocode.

D. IN-BAND WORMHOLE DETECTION

1) ROUND TRIP TIME (RTT) PHASE

This Phase relied on the RTT value based on its hop count. RTT is the amount of time in milliseconds (ms) between the source nodes sending the request and receiving a response message from the destination node. This phase based on the fact that the RTT value between two fake neighbours is considered as a higher value compared to two real neighbours. Time Threshold is proposed to compare it with the expected time (RTT) of a particular node taking into consideration number of hops. Therefore, when the RTT of that node is lower than time threshold, then the node will be assessed and placed in the trusted list and no wormhole node exists in that link. However, when the RTT value for that node is higher than time threshold, then a wormhole link is exist. Therefore the node will be added to the suspicious list and continue with the PDR phase.

Lemma 2: Let sum S = (m x 1) + (m x 2) + ……..+ (m x i) can be written in the form of

$$S = \sum_{i=1}^{n} (m \times i)$$

Proof:

$$S = (m \times 1) + (m \times 2) + \ldots\ldots\ldots + (m \times i)$$
$$S = m(1 + 2 + \ldots\ldots + i)$$
$$S = m \sum_{i=1}^{n} (i)$$
$$S = m \sum_{i=1}^{n} (m \times i)$$

Therefore, each scenario will be calculated as

$$HC = \sum_{i=1}^{i=6} (i \times 25) \tag{5}$$

Lemma 3: $\sum_{i=1}^{n} -\lambda xi + \alpha yi = \sum_{i=1}^{n} (-\lambda xi + \alpha yi)$

Proof: $\sum_{i=1}^{n} -\lambda xi + \sum_{i=1}^{n} \alpha yi = -\lambda x1 + -\lambda x2 + \ldots. + -\lambda xn + \alpha y1 + \alpha y2 + \ldots + \alpha yn = (-\lambda x1 + \alpha y1) + (-\lambda x2 + \alpha y2) + \ldots. + (-\lambda xn + \alpha yn) = \sum_{i=1}^{n} (-\lambda xi + \alpha yi)$

If we assume xi denoted as *Tf*, and yi denoted as *Tb,* the round trip time total (RTT*t*) for each scenario can be calculated to the immediate neighbouring connected node using (5):

$$RTTt = \sum_{n=1}^{n=25} (Tf + Tb) \tag{6}$$

where *Tf* is the time that packet needs to travel from source node to its destination. *Tb*, is the time that packet needs get back to its original source.

Thus, the time threshold obtained using (6) and (5) for each scenario as shown below.

$$\text{Time Threshold} = \frac{RTTt}{HC} \tag{7}$$

2) PACKET DELIVERY RATIO (PDR) PHASE

Third Phase, where all nodes that reach this phase will be examined by their packet delivery ratio (PDR). The nodes that are in the suspicious list will be checked by PDR detection and compare their PDR with the threshold value that is calculated using K-Means clustering algorithm as illustrated in (3). The algorithm processes the input one at a time and tries all possible values of the PDR from 0-1, maintaining these results in their hidden units that implicitly contains information about the history of all the past PDR results. The centroid value (output) of the hidden units is the threshold value of the PDR which will be compare with the PDR of the each node. If it's less than the threshold value, a wormhole node is detected in this route. Otherwise that node is considered a trusted node and no wormhole node exists in the link. Packet delivery ratio threshold pseudocode shown in the Algorithm 3.

However, the three phases manage to increase the efficiency and performance of wormhole attack detection. Each phase achieve a particular form of detection resulting in having the potential to detect malicious nodes. The in-band detection algorithm illustrated in the algorithm 4.

V. SECURITY ANALYSIS OF THE PROPOSED ALGORITHM

Wormhole attacks are able to avoid detection. Where the attacker can temporarily stop sending data at high speed link once it observes the detection event, also the attack can be performed even if the network communication provides confidentiality and cryptography key [46]. HWAD, will overcome security gaps that let the attacker access and distort the network behaviour due to the hybrid detection methods that can performs detection at different phases. These results activate detection of both in-band and out-of-band wormholes even during the network running phase. In this section, we analyse the security of HWAD under these attacks.

Algorithm 3 PDR threshold value using K-Means algorithm

1. Run NS2 simulation.
2. Gather the mobility, trace file and result file that resulted from the previous simulation.
3. Run K-Means Clustering Algorithm
4. Cluster the input file for each node to be run as one element
   Else
5. The algorithm try all possible values for PDR for Node A
6. For all results for Node A:
7. Select PDR with the best result
8. The previous step done for all nodes
9. Now the optimal PRD for each node is ready
10. PDR for all nodes process to find the average optimal PDR for the network
11. End of Pseudocode.

Algorithm 4 In-Band Wormhole Detection Algorithm

Input: RTT threshold, PDR threshold (centroid), number of hops.

Output: in-band detection.

1. Star
2. Nodes are deployed using AODV protocol
3. Star
4. If (RTT > threshold) the
5. Add node to the suspicious list
6. Start
7. If (PDR>= threshold) the
8. No wormhole detected
9. else
10. In-Band wormhole attack
11. else
12. No wormhole detected, add to the trusted list
13. End of Pseudocode.

- In-Band Wormhole: HWAD algorithm performed detection against in-band attack that can be run through packet encapsulation even if the malicious node fabricated its identity. Round trip time employed to generate neighbour information, determine the nearest node to the source and calculate the time required of the packet to travel between successive nodes taking hop count into consideration to determine the suspected wormholes. Next, packet delivery ratio is applied to avoid tampering with the packet while transmission as well as fulfil the maximum number of packet received by the destination. In PDR we employ K-Means machine learning algorithm that provided accurate as well as faster computation for threshold value. Once wormholes perform an attack, the detection algorithms will identify the attacker and prevent malicious node to gain the legitimate path in ad-hoc network.
- Out-of-band Wormhole: this type of attack equipped with long-range directional wireless link and transmission power to let the packet to travel over long distance. Therefore, HWAD perform the detection against this type of attack through measuring the transmission range of each node. Transferring packets through wormhole odes lead to a time delay, this will increase the transmission time. However, Hello Interval used mathematical calculations to measure the transmission range of each nodes as shown in equation (4).

VI. MATHEMATICAL MODEL FOR TIME AND SPACE COMPLEXITY

For MANET that has been constructed based on HWAD algorithm, the time and space complexity calculated theoretically. Time resources usually measured through calculating deployment and required time to solve problems. On the other hand, space resources that is measured through the size of storage and required space to solve problems. The basis for calculating computational complexity is the amount of necessary resources. The effectiveness or complexity of an algorithm is expressed as a function whose domain is the size of the input data, and the range of values is usually the number of steps to be performed for to find out the time as well as space complexity needed.

Lemma 4: The space complexity (SC) result of the HWAD proposed algorithm is O (n*n).

Proof: In creating wireless MANET network constructed on HWAD algorithm, new mobile nodes were added at a constant rate to the algorithm. Hence, it was more appropriate to employ and adopt the adjacency matrix which represents the construction of the network. In HWAD algorithm, the source node needs know range of all nodes to locate the node when it's added the wireless network. Therefore, the space complexity (SC) is O (n*n)

Lemma 5: We next discuss time complexity (TC) of the HWAD proposed algorithm which is O (n).

Proof: The network development progress and its connections are important for determining the time complexity (TC) of HWAD algorithm. Where each new node will join the network will pass through these three processes. In the algorithm, the network start at minimum two connected nodes. The new nodes are allowed to joined the network based on transmission time have inferior time complexity (TC) was $O(n_1)$. On the other hand, the new nodes that will connect later on to the existing network have the inferior time complexity is O(n2). Therefore, $n = n_1 + n_2$ the time complexity of HWAD algorithm is $O(n)$.

VII. SIMULATION SETUP AND PARAMETERS

To evaluate the performance of detection method and accuracy of the proposed approach HWAD. It has been simulated HWAD performance using NS-2 simulator environment on Ubuntu 16.04 LTS operating system. Then, the proposed approach tested under particular parameters which make the system perform best. Table 1 shows the simulation

TABLE 1. List of simulation parameter.

Parameter	Value
Simulator	NS-2.3/ Ubuntu 16.04 LTS
Topological area	100 m x 100 m
Simulation time	500 seconds
Node locations	Randomly
Radio propagation model	Two-ray ground reflection
Bandwidth	2.0 Mbps
Mobility model	Way point
Initial energy	100 Joules
Traffic type	CBR
Packet size	512 bytes
Number of nodes	25 - 150 nodes
HELLO interval	300 milliseconds (NS2 default).

parameters. The performance metrics considered to evaluate the proposed algorithms and analysing performance are throughput, end to end delay, packet delivery ratio, and consumed energy. Moreover, the simulation was carried out under various number of mobile nodes to ensure and prove the efficiency of the proposed approach HWAD in ad-hoc network.

VIII. RESULT COMPARISON AND EVALUATION

In order to evaluate the efficiency of the proposed approach HWAD, we compared its performance with some other well-known wormhole detection approaches in MANET. Such as MCRP algorithm [47] and Aliady and Al-Ahmadi [48] using several network metrics. In the all figures below, the x-axis represents the number of nodes and the y-axis represents the metrics with different network scenarios.

A. PERFORMANCE COMPARISON BETWEEN HWAD WITH ALIADY et al [48] ALGORITHM

1) THROUGHPUT

The graphs in Fig.5 illustrate the improvement gained in throughput in HWAD compared with ALIADY algorithm with various number of nodes (50-150). This plot shows the rate of successfully packet received by destination. The throughput values in HWAD are (149.075, 148.945, 149.843) respectively outperform the ALIADY values that are (149.38, 144.8, 147.7) respectively even when the number of nodes reach to 150 nodes. The reason behind that the ALIADY algorithm based on neighboring information where malicious nodes can fabricate their neighborhood list to manipulate the detection method. Also, the detection will be hard if the tunnel is less than four hops. While the throughput in HWAD remain highest even with different network size. Therefore, HWAD can provide higher performance, quality and successful throughput to the destination compared to the ALIADY.

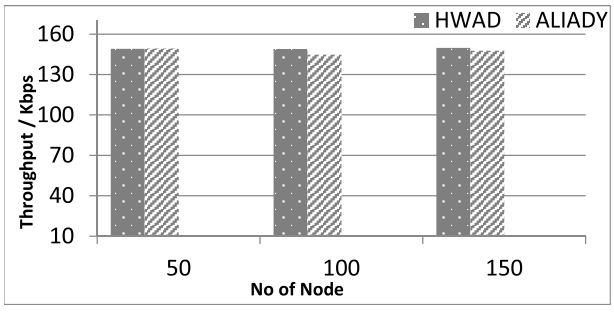

FIGURE 5. Comparison between HWAD and ALIADY *et al* [48] for throughput with wormhole attack.

2) CONSUMED ENERGY

Fig.6 shows the comparison in amount of energy consumption required from the HWAD and ALIADY between (50-150) nodes. The plots describe that HWAD consumes energy (43.59, 43.61, and 40.13) respectively and for ALIADY (175, 80, and 220) joules. Where energy consumption in HWAD within the normal range and is considered less than ALIADY when the network under attack. ALIADY consume additional energy. The reason behind that is the second stage of checking that is require discovering additional neighbours two hops away from the following neighbour to find the intersection with source within 3 hops. HWAD employ (NRT) which will decrease the amount of energy consumed in the network.

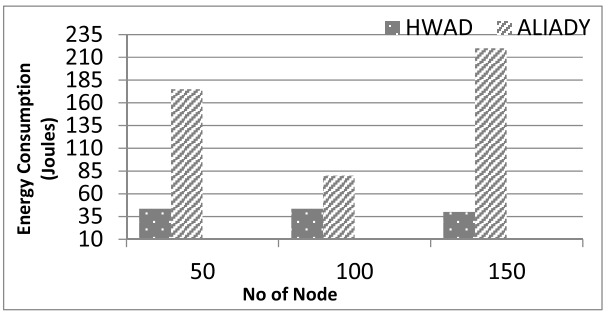

FIGURE 6. Comparison between HWAD and ALIADY *et al* [48] for consumed energy with wormhole attack.

3) END TO END DELAY

Fig.7 presents the packet delay that plays an important role for measuring the network performance. Since minimum delay ensure the quality and performance of transmission. The delay values for HWAD are (0.085, 0.112, 0.253) respectively whereas the delay values in ALIADY are (3.9, 0.9, 2) respectively. The plots show the highest delay in ALIADY at various network density. This is because ALIADY perform two stages of checking between neighbours in the elected path to check whether there is a three hops path to nodes. However, when the network density increase, the HWAD remain with smallest delay compared ALIADY that has negatively impacted performance. It is very clear that the HWAD will ensure the packet can be transmitted in a safe path and short time across the network.

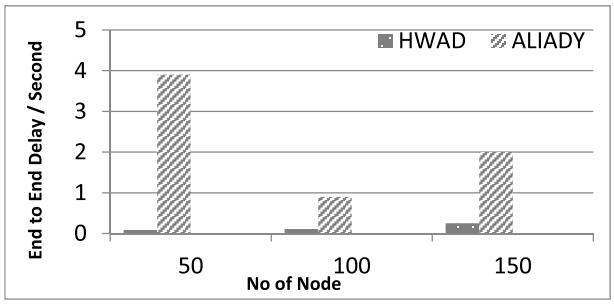

FIGURE 7. Comparison between HWAD and ALIADY *et al* [48] for end to end delay with wormhole attack.

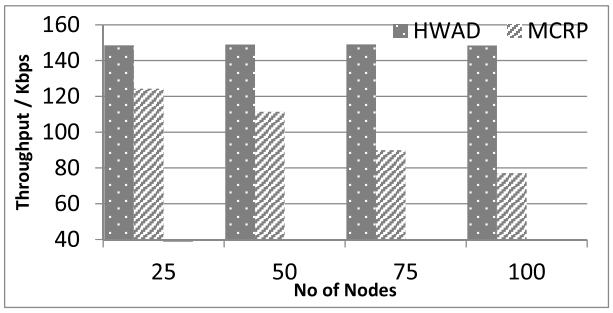

FIGURE 9. Comparison between HWAD and MCRP [47] for throughput with wormhole attack.

B. PERFORMANCE COMPARISON BETWEEN HWAD WITH MCRP [47] ALGORITHM

1) PACKET DELIVERY RATIO

Fig.8 shows the packet delivery ratio and reflects the efficiency and performance of HWAD in the network as compared to MCRP. The plots display HWAD packet delivery results (99.982, 99.972, 98.988, 98.972) respectively is producing the highest packet delivery values for the different network densities compared to MCRP packet delivery results (85, 82, 78, 76) respectively under wormhole attack. When the network density increases, the percentage of packet delivery continuously decreases in MCRP due to the network congestion at base station (BS) as well as increase in the delay resulting BS receive many request from nodes to get the path to the destination, which increase the opportunity of dropping packet. However, HWAD offers improvements to ensure the packet is delivered to the destination by delivering at least 98% packets sent compared with 76% MCRP. HWAD was able to mitigate the attack while transmission occurs within the same area.

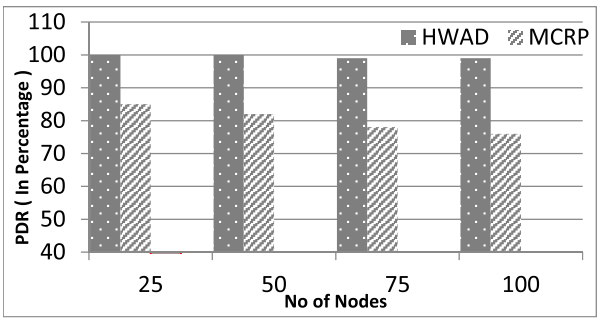

FIGURE 8. Comparison between HWAD and MCRP [47] for packet delivery ratio with wormhole attack.

2) THROUGHPUT

The graphs in Fig.9 show the comparison between HWAD and MCRP in throughput. The plots prove that, the HWAD gain throughput results are (148.51, 149.01, 149.12, 148.48) respectively outperforms MCRP throughput results (124.28, 111.42, 90, 77.1) respectively at different scenarios. The results shows a significant decrease in the MCRP throughput while the network density increase due to increase in the delay, high traffic and many requests to the BS which reflect negatively on the network performance. Also, the packet pass through long wormhole tunnel which will lower the throughput in MCRP. However, HWAD perform better than MCRP in throughput because each node reliably passes the largest amount of packets which will increases the network performance

3) END TO END DELAY

Fig.10 shows the end-to-end delay through different network size. The plots show a small increases in the delay in HWAD are (0.081, 0.085, 0.09, 0.099) respectively whenever the size of the network increase. While, the delay are (0.15, 0.4, 0.9, 1.5) respectively for MCRP algorithm. However, HWAD remains with smallest delay because the packets does not pass through wormhole tunnel compared with MCRP which has a vast delay whenever the network nodes increase due to many tasks performed by BS to the network nodes such as calculate and deliver routing paths to the nodes. Also, the packet travel through the wormhole tunnel in case of the instant ratio of T_c and T_m is less than the average ratio resulting in higher delay. It is very clear that the HWAD will ensure the packet can be transmitted in a safe path and short time.

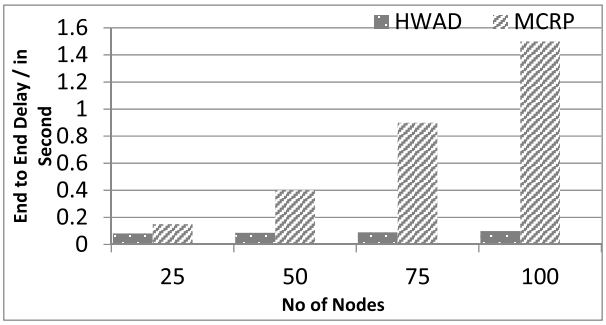

FIGURE 10. Comparison between HWAD and MCRP [47] for end to end delay with wormhole attack.

IX. CONCLUSION AND FUTURE WORK

A hybrid wormhole attack detection (HWAD) algorithm in MANET able to detect two types of wormhole attack, in-band wormhole using round trip time and packet delivery ratio

that used K-Means clustering algorithm. While out-of-band wormhole uses transmission range between successive nodes. HWAD was proposed to enhance the wormhole attack detection for both types, in-band and out-of-band. Neighbour ratio threshold helped to lower the energy consumption and delay through reducing the number of detection nodes. This algorithm is applied on the AODV protocol and implemented using NS-2 simulator to measure different parameters for various number of nodes with different metrics. The simulation of the proposed algorithm outcomes have clearly proved that the proposed approach has higher performance, more effective and detection accuracy over compared algorithms in several metrics such as throughput, packet delivery ratio, end to end delay and consuming energy. HWAD detection approach ensures that the wormhole attack is treated for both types in-band and out-of-band attack. However, the proposed algorithm in general outperformed other algorithms in a set of measured parameters.

In the future we will focus on using Ad-hoc network in a large size topological area which provided greater flexibility and more accurate detection performance in wireless networks. In addition, we will overcome the consuming energy due to the limited energy supply of mobile node. It is of the utmost importance to focus of study on wormhole attack detection, as it enables us through seeking out more possible techniques to counteract the attack in our future research, in order to apply HWAD to more complex condition.

REFERENCES

[1] S. Majumder and D. Bhattacharyya, "Mitigating wormhole attack in MANET using absolute deviation statistical approach," in *Proc. IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2018, pp. 317–320.

[2] J. Seo and G. Lee, "An effective wormhole attack defence method for a smart meter mesh network in an intelligent power grid," *Int. J. Adv. Robot. Syst.*, vol. 9, p. 49, Dec. 2012.

[3] S. Amutha and K. Balasubramanian, "Secured energy optimized ad hoc on-demand distance vector routing protocol," *Comput. Electr. Eng.*, vol. 72, pp. 766–773, Nov. 2018.

[4] S. Rezaei, M. Gharib, and A. Movaghar, "Throughput analysis of IEEE 802.11 multi-hop wireless networks with routing consideration: A general framework," *IEEE Trans. Commun.*, vol. 66, no. 11, pp. 5430–5443, Nov. 2018, doi: 10.1109/TCOMM.2018.2848905.

[5] M. Zaminkar and R. Fotohi, "SoS-RPL: Securing Internet of Things against sinkhole attack using RPL protocol-based node rating and ranking mechanism," *Wireless Pers. Commun.*, vol. 114, no. 2, pp. 1287–1312, Sep. 2020.

[6] A. Amara korba, M. Nafaa, and S. Ghanemi, "Analysis of security attacks in AODV," in *Proc. Int. Conf. Multimedia Comput. Syst. (ICMCS)*, Marrakech, Morocco, 2014, pp. 752–756, doi: 10.1109/ICMCS.2014.6911193.

[7] R. Singh, J. Singh, and R. Singh, "WRHT: A hybrid technique for detection of wormhole attack in wireless sensor networks," *Mobile Inf. Syst.*, vol. 2016, Jan. 2016, Art. no. 8354930.

[8] S. R. M. Jamali; Fotohi; Analoui, "An artificial immune system based method for defense against wormhole attack in mobile ad hoc networks," *Tabriz J. Electr. Eng.*, vol. 47, 4, 2018, pp. 1407–1419.

[9] J. Li, D. Wang, and Y. Wang, "Security DV-hop localisation algorithm against wormhole attack in wireless sensor network," *IET Wireless Sensor Syst.*, vol. 8, no. 2, pp. 68–75, Apr. 2018, doi: 10.1049/iet-wss.2017.0075.

[10] Z. Shi, R. Sun, R. Lu, J. Qiao, J. Chen, and X. Shen, "A wormhole attack resistant neighbor discovery scheme with RDMA protocol for 60 GHz directional network," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 341–352, Dec. 2013, doi: 10.1109/TETC.2013.2273220.

[11] S. Qazi, R. Raad, Y. Mu, and W. Susilo, "Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks," *J. Inf. Secur. Appl.*, vol. 39, pp. 31–40, Apr. 2018.

[12] P. Lee, A. Clark, L. Bushnell, and R. Poovendran, "A passivity framework for modeling and mitigating wormhole attacks on networked control systems," *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3224–3237, Dec. 2014, doi: 10.1109/TAC.2014.2351871.

[13] R. W. Anwar, M. Bakhtiari, A. Zainal, A. H. Abdullah, and K. N. Qureshi, "Enhanced trust aware routing against wormhole attacks in wireless sensor networks," in *Proc. Int. Conf. Smart Sensors Appl. (ICSSA)*, Kuala Lumpur, Malaysia, May 2015, pp. 56–59, doi: 10.1109/ICSSA.2015.7322510.

[14] S. Shukla and S. Naganna, "A review on K-means data clustering approach," *Int. J. Inf. Comput. Technol.*, vol. 4, no. 17, pp. 1847–1860, 2014.

[15] H. Sun Chiu and K.-S. Lui, "DelPHI: Wormhole detection mechanism for ad hoc wireless networks," in *Proc. 1st Int. Symp. Wireless Pervas. Comput.*, Phuket, Thailand, 2006, p. 6, doi: 10.1109/ISWPC.2006.1613586.

[16] P. Amish and V. Vaghela, "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol," in *Proc. 7th Int. Conf. Commun., Comput. Virtualization*, 2016, pp. 700–707.

[17] Z. Tun and A. Maw, "Wormhole attack detection in wireless sensor networks," *Int. J. Elect., Comput., Energetic, Electron. Commun. Eng.*, vol. 2, no. 10, p. 46, 2008.

[18] S. Äapkun, L. Buttyán, and J.-P. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," in *Proc. 1st ACM workshop Secur. Ad Hoc Sensor Netw. (SASN)*, Washington, DC, USA, 2003, pp. 21–32.

[19] G.-H. Lai, "Detection of wormhole attacks on IPv6 mobility-based wireless sensor network," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, p. 274, Dec. 2016.

[20] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 370–380, Feb. 2006, doi: 10.1109/JSAC.2005.861394.

[21] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, CA, USA, Feb. 2004, pp. 241–245.

[22] H. Chen, W. Lou, X. Sun, and Z. Wang, "A secure localization approach against wormhole attacks using distance consistency," *EURASIP J. Wireless Commun. Netw.*, vol. 2010, no. 1, Dec. 2009, Art. no. 627039, doi: 10.1155/2010/627039.

[23] S. Jamali and R. Fotohi, "Defending against wormhole attack in MANET using an artificial immune system," *New Rev. Inf. Netw.*, vol. 21, no. 2, pp. 79–100, Jul. 2016.

[24] N. Tamilarasi and S. G. Santhi, "Detection of wormhole attack and secure path selection in wireless sensor network," *Wireless Pers. Commun.*, vol. 114, pp. 329–345, Sep. 2020.

[25] S. Sankara Narayanan and G. Murugaboopathi, "Modified secure AODV protocol to prevent wormhole attack in MANET," *Concurrency Comput., Pract. Exper.*, vol. 32, no. 4, Feb. 2020, Art. no. e5017, doi: 10.1002/cpe.5017.

[26] S. Jamali and R. Fotohi, "DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system," *J. Supercomput.*, vol. 73, no. 12, pp. 5173–5196, Dec. 2017.

[27] A. Aswale and R. Joshi, "Security enhancement by preventing wormhole attack in MANET," in *Innovation in Electronics and Communication Engineerin*, vol. 237. Singapore, Springer, 2020, p. 255.

[28] R. Fotohi, E. Nazemi, and F. Aliee, "Anagent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks," *Veh. Commun.*, vol. 26, May 2020, Art. no. 100267.

[29] D. Kaur and P. Singh, "Various OSI layer attacks and countermeasure to enhance the performance of WSNs during wormhole attack," *ACEEE Int. J. Netw. Secur.*, vol. 5, no. 1, p. 62, Jan. 2014.

[30] T. Bin, L. Qi, Y, Yi-xian, L. Dong, and X. Yang, "A ranging based scheme for detecting the wormhole attack in wireless sensor networks," *J. China Univ. Posts Telecommun.*, vol. 19, pp. 6–10, Sep. 2012, doi: 10.1016/S1005-8885(11)60478-0.

[31] S. Ji, T. Chen, and S. Zhong, "Wormhole attack detection algorithms in wireless network coding systems," *IEEE Trans. Mobile Comput.*, vol. 14, no. 3, pp. 660–674, Mar. 2015, doi: 10.1109/TMC.2014.2324572.

[32] S. Gupta, S. Kar, and S. Dharmaraja, "WHOP: Wormhole attack detection protocol using hound packet," in *Proc. Int. Conf. Innov. Inf. Technol.*, Abu Dhabi, United Arab Emirates, 2011, pp. 226–231, doi: 10.1109/INNOVATIONS.2011.5893822.

[33] M. Okunlola, A. Siddiqui, and A. Karami, "A wormhole attack detection and prevention technique in wireless sensor networks," *Int. J. Comput. Appl.*, vol. 174, no. 4, pp. 1–8, Sep. 2017.
[34] L. Lu, M. J. Hussain, G. Luo, and Z. Han, "Pworm: Passive and real-time wormhole detection scheme for WSNs," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 11, Nov. 2015, Art. no. 356382.
[35] M. Azer, S, El-Kassas, and M. El-Soudani, "Towards introducing complex wormhole attacks in wireless ad hoc networks," *Int. J. Comput. Sci. Inf. Secur.*, vol. 1, no. 1, pp. 354–373, May 2009.
[36] S. Ali, P. Nand, and S. Tiwari, "Impact of wormhole attack on AODV routing protocol in vehicular ad-hoc network over real map with detection and prevention approach," *Int. J. Vehicle Inf. Commun. Syst.*, vol. 5, no. 3, p. 354, 2020.
[37] D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," *IEEE/ACM Trans. Netw.*, vol. 19, no. 6, pp. 1787–1796, Dec. 2011, doi: 10.1109/TNET.2011.2163730.
[38] J. Anju and C. N. Sminesh, "An improved clustering-based approach for wormhole attack detection in MANET," *Int. Conf. Eco-Friendly Comput. Commun. Syst.*, Mangalore, Karnataka, 2014, pp. 149–154, doi: 10.1109.2014.
[39] S. Eidie, B. Akbari, and P. Poshtiban, "WANI: Wormhole avoidance using neighbor information," in *Proc. 7th Conf. Inf. Knowl. Technol. (IKT)*, Urmia, Iran, May 2015, pp. 1–6, doi: 10.1109/IKT.2015.7288750.
[40] S. Khobragade and P. Padiya, "Detection and prevention of wormhole attack based on delay per hop technique for wireless mobile ad-hoc network," in *Proc. Int. Conf. Signal Process., Commun., Power Embedded Syst. (SCOPES)*, Paralakhemundi, Odisha, Oct. 2016, pp. 1332–1339, doi: 10.1109/SCOPES.2016.7955657.
[41] P. Parvathi, "Comparative analysis of CBRP, AODV, DSDV routing protocols in mobile Ad-hoc networks," in *Proc. Int. Conf. Comput., Commun. Appl.*, Dindigul, India, vol. 2012, pp. 1–4, doi: 10.1109/ICCCA.2012.6179145.
[42] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map," *IEEE Access*, vol. 7, pp. 95197–95211, 2019, doi: 10.1109/ACCESS.2019.2928804.
[43] J. Qi, Y. Yu, L. Wang, and J. Liu, "K-means: An effective and efficient K-means clustering algorithm," in *Proc. IEEE Int. Conferences Big Data Cloud Comput. (BDCloud)*, Atlanta, GA, USA, Oct. 2016, pp. 242–249, doi: 10.1109/BDCloud-SocialCom-SustainCom.2016.46.
[44] N. Dhaachandra, K. Manglem, and Y. Chanu, "Image segmentation using K-means clustering algorithm and subtractive clustering algorithm," in *Proc. Int. Multi-Conf. Inf. Process.*, 2015, pp. 764–771.
[45] C. Yuan and H. Yang, "Research on K-value selection method of K-means clustering algorithm," *Sci. J.*, vol. 2, no. 2, pp. 226–235, Jun. 2019, doi: 10.3390/j2020016.
[46] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. 23nd Annu. Joint Conf. Comput. Commun. Soc.*, San Francisco, CA, USA, 2003, pp. 1976–1986, doi: 10.1109/INFCOM.2003.1209219.
[47] O. R. Ahutu and H. El-Ocla, "Centralized routing protocol for detecting wormhole attacks in wireless sensor networks," *IEEE Access*, vol. 8, pp. 63270–63282, 2020, doi: 10.1109/ACCESS.2020.2983438.
[48] W. A. Aliady and S. A. Al-Ahmadi, "Energy preserving secure measure against wormhole attack in wireless sensor networks," *IEEE Access*, vol. 7, pp. 84132–84141, 2019, doi: 10.1109/ACCESS.2019.2924283.

MUHANNAD TAHBOUSH was born in Amman, Jordan. He received the bachelor's degree in computer engineering from Near East University, North Cyprus, in 2003, and the master's degree in computer science from DePaul University, in 2008. He is currently pursuing the Ph.D. degree in computer engineering with Cyprus International University, Nicosia, North Cyprus. His research interests include network security, cryptography, and data communication.

MARY AGOYI received the Ph.D. degree in computer engineering. She is currently an Assistant Professor with Cyprus International University. Her research interests include networking, information security, and image watermarking.