IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 13, 2019, accepted June 17, 2019, date of publication June 21, 2019, date of current version July 12, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2924283

Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Networks

WATEEN A. ALIADY AND SAAD A. AL-AHMADI
Computer Science Department, King Saud University, Riyadh 11362, Saudi Arabia

Corresponding author: Wateen A. Aliady (437202947@student.ksu.edu.sa)

This work was financially supported by the Deanship of Scientific Research at King Saud University through the initiative of the DSR Graduate Students Research Support (GSR).

ABSTRACT A wireless sensor network consists of sensors having autonomous wireless communication with the ability to sense their surrounding conditions and an ability to connect to the Internet through a base station. In most cases, sensors are spatially distributed and, hence, must have a low cost; for this reason, they have limited batteries, computational ability, and memory size. Sensors' restrained ability to implement common security measures makes them vulnerable to various types of attacks. Moreover, their applications are sensitive to delay or packets corruption, e.g., forest fire detection, disaster relief operations, and lots of other applications. Therefore, improving security is compulsory. There are various types of attacks targeting different network layers. One type is a wormhole attack that is a harmful and easily deployed attack that targets the routing layer. In this paper, a proposed energy preserving secure measure based on the network connectivity aims to detect the wormhole attack. The proposed measure is applied to the ad-hoc on-demand distance vector routing protocol and the experiment is tested using Network Simulator 3. The results state that the detection accuracy is 100% when the wormhole tunnel is of four hops or more in length. In addition, the method has no additional costs because it is not based on any plugged hardware, e.g., synchronized clocks or geographical positing system, as this makes this method appealing for the wireless sensor network environments.

INDEX TERMS Ad-hoc on-demand distance vector routing protocol, sensors, network simulator 3, wireless sensor network, wormhole attack.

I. INTRODUCTION

In recent decades, Wireless Sensor Networks (WSNs) have gained increasing interest within research communities for its major role in wide number of applications. It makes life more convenient, safe and easy. Moreover, it is adapted in variant areas e.g., health, environment, traffic, surveillance and industry. It also lacks infrastructure and is composed of sensor nodes that can communicate directly through a transceiver [1].

It is composed of sensors that can sense their surrounding environment, to deliver the information to a base station that has a connection to the Internet as shown in Fig. 1 the base station has more computational and storage abilities than sensors. The sensed information is sent through the base station to be received for those of interest. For example, habitat and environment monitoring is of interest to scientists and researchers interested in natural sciences [2].

A sensor is composed of a sensing unit to sense the environment, a processing unit, storage, a transceiver unit to communicate, a power unit used for power supply.

There are optional units in a sensor which are: location finding system to determine the sensor's location, a power generator, and a mobilizer that is needed to move sensor nodes when required to carry out a specific task [3].

In pursuance to implement, there are some challenges that are required to be solved. The major challenge in adapting this type of network is preserving energy because sensors have limited life time. Furthermore, sensors have limited storage space and restricted computational ability and thus making defense against security attacks more challenging [4].

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

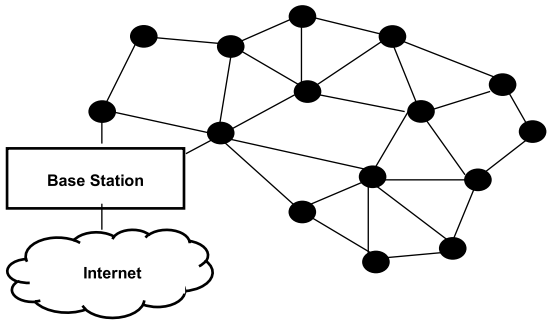

FIGURE 1. Wireless sensor networks.

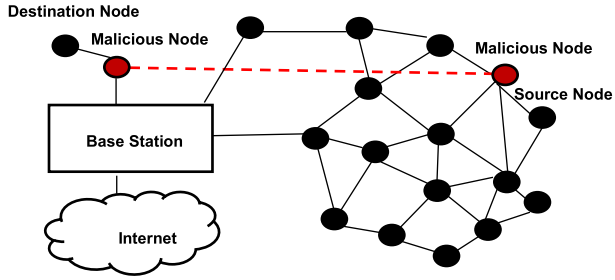

FIGURE 2. Wormhole attack in wireless sensor network.

Security is a priority in wide applications e.g., responding to emergency as in natural disasters, military and in safety critical operations. If communication is damaged catastrophes might happen without the rescue team's knowledge. There are many types of security attacks that target routing protocols in WSNs referred to as routing attack e.g., Sybil, wormholes and spoofing attacks [5].

Wormhole attack is described as generating untrusted shortcut through the network. This is formed when two intruder sensors have a higher transmission range ability than normal sensors. They can form direct communication between them which is equal to the length of the distance between them as shown in Fig.2. Also, they can communicate with the rest of the normal sensors using the normal sensor's standard transmission range. The first malicious sensor eavesdrops on one location to receive and tunnel packets to the second malicious sensor. Afterwards, the second sensor forwards the received packets to the intended destination. Alternatively, the malicious sensor has the capability to capture the packets within a certain area and send them to other remotely placed sensors. Because packets generated by malicious sensors are received earlier than packets generated by normal sensors, the destination sensor will drop the normal packets. The major problem of the wormhole attack is that it can be effortlessly started by the intruder without the need of understanding the network or applying cryptographic techniques [6], [7] and [8].

It is shown in Fig. 2 the generated wormhole tunnel by two intruder sensors. They use this tunnel to not allow any legitimate sensor to receive the transmitted packets. This way they ensure that their packets will be received earlier. Therefore, they can control the transmitted packets by either altering or dropping them.

Wormhole attack is among the most extreme routing attacks, which can be implemented easily yet hard to detect. This attack can be launched regardless if the host is being compromised or not, even if the network assures authenticity and confidentiality. They can affect the network by changing or dropping the sent packets or just by collecting a substantial number of packets with the goal of traffic examination or encryption breaking. It can influence the system to make it powerless in discovering routes that are longer than two hops thus this will result in giving a false network topology [9].

This work contributes in securing Wireless Sensor Networks against wormhole attack by proposing an energy preserving secure measure. One of the least explored performance measures in existing secure methods is energy consumption. Therefore, energy performance is the main concern in this work to ensure that the network will have a long-life time. Sensors have limited energy and usually they operate on batteries. It is difficult to change their batteries every now and then because they are distributed or implemented randomly and in a harsh environment. To achieve limited energy consumption, the detecting method must not have a high computational need to be able to perform. High computations e.g., cryptography will drain sensors battery in no time. Furthermore, the proposed method must limit the additional costs to the sensors' implementation because there is a massive number of sensors in the field. Therefore, using additional hardware e.g., Geographical Positing System (GPS), guard nodes, synchronized clocks or any additional equipment will be costly. The following section includes a review of some existing detection methods.

The rest of this paper is structured as follows. Section 2 presents related work of existing detection methods. Section 3 introduces the proposed secured method. Section 4 discusses simulation parameters and evaluation performance. Finally, Section 5 concludes.

II. RELATED WORK

A review of the existing work of wormhole attack detection methods is presented in this section as each security method could be categorized under one or more of these categories: Round Trip Time (RTT), hop count, geographical information, Received Signal Strength Indicator (RSSI), statistics, and neighborhood lists. The following describes existing methods and their limitations.

A. TECHNIQUES BASED ON ROUND TRIP TIME

The round-trip time is the time it takes for the packet to be sent and for the acknowledgment to be received. The work in [10], [11] and [12] is based on RTT for detecting this attack. None of these papers presented the detection rate for their method, which is the basic parameter to specify the effectiveness of the proposed method. The limitation for this method is that all sensors in the network must have a tightly

synchronized clock but it is a difficult and expensive task to implement synchronized clocks [13].

Ahmed *et al.* [10] focus is to secure the energy efficient Cross-Layer Medium Access Control (CL-MAC) protocol in WSNs. The CL-MAC is made of two neighboring layers. The MAC layer and network layer that trade control packets to locate the shortest route to the base station with the goal that every node having a place with the same path must be prepared for routing packets. Other nodes which are neighbors and do not have a place with the path need to go to a sleeping phase, turn off their transceiver, from the starting point to the finish of the routing procedure. The attack can take place as in the following scenario, a malicious node tunnels a Request To Send (RTS) packet that is sent from one zone to a zone in the distance, to put all nodes in this remote zone into sleep mode. This paper has proposed a solution that differentiates between the passive and active wormhole attacks as it gives each a different solution. In the passive attack which is when packets are not modified, the RTT is calculated. This is calculated in the network layer by route request and route reply messages. In addition to this, it is calculated in the MAC layer while sending hello messages periodically to build neighbors list. In the active attack, the communication is protected by adding a flag variable to specify if the receiver is suitable. The limitation for this method is that it consumes more energy if the wormhole node is remotely located from the sink.

Amish and Vaghela [11] propose security against wormhole attack in Ad-hoc On-demand Multipath Distance Vector routing protocol (AOMDV) that is an extension to Ad-hoc On-demand Distance Vector routing protocol (AODV). The paper mentions that for two sensors to communicate, the sender investigates if there is a path to the destination in its own routing table. If a route is not presented it broadcasts a RREQ packet to its neighbors, as the neighbors in turn check for a route or forward the RREQ until the destination is discovered. Afterwards, the destination generates a Route Reply (RREP) packet to the source following the exact route for the received RREQ. For every received RREQ in the destination a route is generated and saved in the routing table of the source. The proposed method calculates the RTT for each generated route by noticing the time when the sender sends RREQ and it receives RREP. Afterwards, it divides each RTT by corresponding hop count and the average value is a threshold value. If the RTT is less than this threshold and number of hops are two, then a wormhole exists. This solution is able to detect most wormholes with a high throughput and delivery ratio.

Minohara and Nishiyama [12] propose a method to identify wormhole attack on WSNs in a duty-cycling operation, nodes in such operation will periodically sleep to reduce power consumption. It states that synchronous communication is better than the asynchronous communication since it does not require a preamble signal that must be sent before the message. The paper proposes a wormhole attack detection method based on delay observed in synchronized communication. The detection in synchronization protocols is by using the flooding mechanism where the source node sends its time stamp through several paths. At the receiver's side, if the time delta between different paths are different then wormhole is detected. In addition, as the base station receives the packet it checks for the delay if it mismatches hop count, then a wormhole is detected.

B. TECHNIQUES BASED ON HOP COUNT

To detect a wormhole the hop count could be used as the basis of the method as in [14] it was compared to the delay time. In contrast, [15] shows that the hop count was used alone to determine the legitimacy of a node. The limitation for these methods is that it may neglect the legitimate route that is the shortest path to the destination [13]. In addition, paper [15] is based on delay time that requires the nodes to contain a synchronized clock.

Rai *et al.* [14] propose a method of identification in mobile ad-hoc networks. The method is based on the calculation of delay and hop count for several paths chosen randomly. First, one of the nodes in the path was chosen to transmit a packet. Then, a timer was started to measure delay and hop count. The process was repeated and on each iteration the route information associated with its hop count and delay was stored. If the same route appears to have less delay in comparison to other routes, then a certain node is malicious. To detect it, the node that is not encountered previously is found.

Patidar and Dubey [15] proposed an AODV enhancement that works as a defence against black hole and wormhole attacks. It is based on intruder detection system (IDS) agent to detect unusual event in the system by monitoring audit data and reporting alarm in case of a problem. Also, using hop count of different routes to detect a malicious route that has smaller number of hops than other routes. IDS-AODV has better performance than AODV under wormhole attack. The drawback here is adding IDS agent is costly.

C. TECHNIQUES BASED ON GEOGRAPHICAL INFORMATION

A wormhole attack could be identified by geographic information, the location of a sensor. It is clear from the stated that the detection is based on whether the distance is realistic in a certain scenario. In [16] and [17] the proposed methods are based on the distance information of the sensors. Paper [18] takes energy into account when designing the proposed methods. In general, the drawback of this method is that combining a GPS to a sensor is costly.

Sookhak *et al.* [16] propose a method that starts as the sender generates a pairwise key using hash function for both public and private keys. The goal is to send a beacon packet containing location, nodes' ID and destination to its neighbors to generate neighborhood table. In addition, the beacon packet contains a list of private keys to detect malicious nodes. Then, select the best neighbor that is the closest to the destination and must have at least one private key matrix similar to a private key matrix in the sender's

neighborhood table. After that, generate a shared key using the private key to assure the sender of the trustworthiness of the received neighbor. The final step happens in the destination, which is to double check by calculating the distance through path and its relationship with number of hops and transmission range for sensor nodes. The proposed method can detect wormhole attacks with a high accuracy but in a dense environment it is a memory drainage method because this means a large neighborhood table needs to be stored.

Chen *et al.* [17] proposed an identification technique based on mobile beacon. The paper focus is to detect wormhole and localize them based on the network model assumption of having a mobile beacon node that has GPS, static beacon that are fixed in location in advance and static sensors. The drawback to this method is that employment of mobile beacon node is costly. The scheme of detecting a wormhole is to check if there are violations. From the packets' side, its uniqueness property which is identified in that the receiving node should receive a packet once, if a duplicate is received then a wormhole is detected. Second, is from the nodes' side, it checks for violation to transmission constraint Property identified by an existing communication between neighboring nodes that are more apart than their transmission range.

Jegan and Samundiswary [18] proposed a mechanism in Zigbee WSNs using IDS. The paper introduced an Energy Efficient Intrusion Detection System (EE-IDS) that detects wormhole attack in an energy efficient manner in Zigbee based WSNs. First, the sink does a topology discovery for all nodes as it broadcasts topology discovery message to nodes that will do measure quality of service e.g., residual energy and queue delay. Then, fill in the topology information table. Afterwards, give an optimal location for watchdog nodes to have less energy consumption and stronger security. Finally, detect wormholes in watchdog nodes by verifying the trustworthiness of nodes and abnormality in packet delivery ratio.

D. TECHNIQUES BASED ON RECEIVED SIGNAL STRENGTH INDICATOR

Paper [19] and [20] both are based on RSSI to detect wormholes, which is a property check based on signal attenuation, that is based on the idea of the malicious node being further in distance than the rest neighbors therefore the responded message must have less signal strength in the malicious neighbor than in the normal neighbors. Based on the previous information the sender detects this node as malicious node. Some malicious node can fabricate the RSSI [19].

Krentz and Wunder [19] proposed a method that is totally based on the RSSI to avoid hidden wormholes using channel reciprocity. This paper proposed a Secure Channel REciprocity-based WormholE Detection (SCREWED), that has two operations. The first method is called Sampling which is based on sending N pings and pongs between two nodes, that is node A sends N pings to node B, and node B replies with pongs. A timeout for these is added to avoid deadlock such as when certain ping or pong is lost. Those are sent using channel hopping to generate variation in RSSI. The second operation is called judgment that is node A sends a judge message to B, so node B shall decide if node A should be dropped or not based on received pongs, and RSSI correlation of node A and B.

In [20] it can trigger a wormhole link by two checking methods. The first is based on the RSSI and the second method is to overcome the first method drawback that some malicious nodes can fabricate the RSSI. This method is based on the RTT, to measure the time for a packet to be transmitted between two neighbors. If the time is less than the average RTT of all neighbors, then a wormhole link is detected.

E. TECHNIQUES BASED ON STATISTICS

A wormhole can be detected using statistics e.g., in [21] as it builds clusters for nodes on time arrival basis. In addition, [22] presented a method that relies on online outlier detection algorithm. as these methods are explained below under the techniques based on neighborhood lists section because they belong under two techniques. The limitation here is the need for power, memory and computing capability of sensor nodes makes it inefficient to implement such advanced algorithms [13].

F. TECHNIQUES BASED NEIGHBORING LISTS

A good detection method could be based on building a neighborhood list as in [23], [21] and [24] but with some variations. This method is usually dependent on the network connectivity, thus having a dense network gives a better result. In the same manner, if the network is dense such that each node has a lot of neighbors, it will consume processing power and memory to analyze the neighborhood lists.

The paper with the title "A ranging based scheme for detecting the wormhole attack in Wireless Sensor Networks" [23] is formulated on the analysis of statics that can identify hidden wormhole attacks. The paper exanimated the node's timing from sending a packet to other nodes until it gets a response which is called an echo for the message. In different words, every node saves the initial timing T and sends out a HELLO packet for neighbor disclosure. Every sensor that gets a HELLO packet transmits an answer. Every sensor assembles its neighbors table that may incorporate distanced neighbors associated with wormholes and calculate the time of arrive (ToA). A formed list is used as an input to the proposed method. It includes the node's identity and the node's ToA. A decision is made, if there was an increase in density above threshold there would be an intrusion detection investigation. If this is the case, then a wormhole detection is performed based on k-means clustering. The ToA is picked as the measure of dissimilarity. In this paper, k is equivalent to two. Clearly the normal and intruder neighbors will have a total of two groups. The detection here reaches 100% when the wormhole tunnel is of 10 hops in length.

The paper [21] proposed a technique for detection that is based on topologies in WSNs. It is constructed on investigating the anomalous arrangement presented by this attack. Every sensor gathers the data of its k-hop neighbors and

their subgraph. At that point, it builds an estimation distance matrix. Next, the matrix of estimation distance is utilized to rebuild the subgraph. Then, insert it on a plane by multidimensional scaling (MDS) amid which every sensor will be allotted a virtual position. The fundamental thought of this wormhole discovery approach depends on an imperative perception as following. If a node is a regular sensor, the MDS format fits with the estimation distance but if a node is an intruder, its neighbor's subgraph cannot be easily inserted on a plane.

Paper by [24] proposed an identification for this attack in mobile WSNs named Statistical Wormhole detection utilizing Neighbors (SWAN). SWAN is a localized method to catch a wormhole. Therefore, it is lighter than the original centralized method. It is persuaded to use the node portability itself to recognize irregularity generated by wormholes. For instance, when a sensor changes its position to a wormhole assault territory and because of the tunnel made by intruder sensors, the sensor would encounter the fast difference in its neighboring nodes attributes. The irregularity is recognized as a sign of an attack by an online outlier detection algorithm because it is founded on the basis of neighboring information, SWAN operates without the need of any exceptional hardware. The proposed SWAN calculation is an approach to identify wormholes based on adjustments in the measurements of the neighborhood data of the past histories, named a training set (Strain) and later samples called a test set (Stest). While versatile sensor node moves towards the area of a malicious node it is going to receive a recent beacon from the neighbors in its transmission range correspondence and from the sensor nodes around the wormhole nodes because of the virtual passage. Each versatile node uses the proposed SWAN algorithm to distinguish intruder nodes.

III. PROPOSED MECHANISM TO DETECT AND PREVENT WORMHOLE ATTACK

This section described the proposed method and analyze it. In addition, it presents its strengths and limitations.

A. THE PROPOSED METHOD OVERVIEW

The proposed method in this paper is based on connectivity and neighborhood information. The method is only performed by sensors of the elected transmission path and their neighbors so that energy consumption and network overhead is reduced.

The method starts during the route reply packet transmission which is a packet used to tell the sender that the path is discovered. The destination sensor is the starting point.

The method is performed between adjacent sensors. First it is applied between the destination and sensor A, then between sensor A and sensor B, afterwards between sensor B and the sender.

Adjacent sensors that could communicate directly search for an alternative short path between them with a maximum length of only three hops as shown in Fig.3,

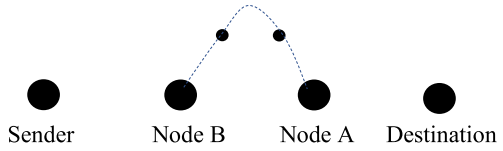

FIGURE 3. Short path between neighboring sensors in the elected path for transmission.

(between sensor A and sensor B). The alternative short path is searched for by using neighborhood lists.

The proposed method is based on two stages of checking that is performed between neighboring sensors in the elected path. Suppose the sending sensor in the elected path is A and the recipient of A is B, B is the following sensor to A in the path. The two stages of checking are performed between A and B. Passing the first stage means it is legitimate and there is no need to go through the second stage as shown in Algorithm 1.

The first stage of checking is to build a first hop neighborhood table for A and a first hop neighborhood table for B. Then, to check if there is a common sensor between the two tables. If not, it goes through the second stage of checking. In the second stage, A checks whether there is a three hops path to sensor B as well as B doing the same. This is done by A using the one hop neighborhood list it had built in the first stage. While, B builds its two hop neighborhood list. B builds it by requesting every sensor in its previous one hop neighborhood list to send their individual one hop neighborhood lists. Then A and B search for an intersection.

Algorithm 1 Secured AODV Routing Protocol Against Wormholes

$N(A)^k$ = k-hop neighbor list of sensor A, where A stands for any sensor in the elected path of transmission.
$N(B)^k$ = k-hop neighbor list of sensor B, where B stands for the next sensor in path, that comes after sensor A.
M = Malicious sensor list.
Input: $N(A)^k$, $N(B)^k$
Output: M

```
for each node A and its adjacent node B do
    if N(A)^1 ∩ N(B)^1 then
        Legitimate
    Else If N(A)^1 ∩ N(B)^2 then
        Legitimate
    Else
        Malicious
        Add A and B to M
Broadcast M
```

B. ANALYSIS

First of all, an analysis of the detection rate based on the proposed method is presented in the following where Fig. 4 describes the detection accuracy of the first stage and Fig. 5 describes the detection accuracy of the second stage.

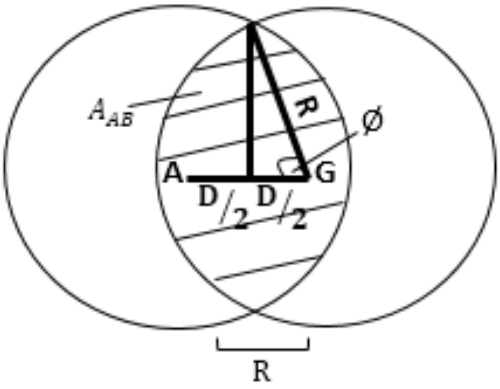

FIGURE 4. Detection accuracy of the first stage.

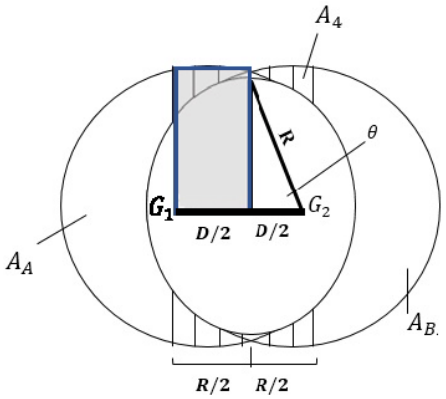

FIGURE 5. Detection accuracy of the second stage.

In Fig. 4, sensor G is in the center of the right circle and sensor A is in the center of the left circle. Moreover, G is a common neighbor sensor for sensors A and B. Furthermore, G is distanced from sensor A within this range D ∈ [0,R] where R is the transmission range. A_{AB} is the area that sensor A and sensor B should exist in, to not be malicious. If sensor B resides in the highlighted area, A_{AB}, then both sensors A and B are not malicious.

However, sensor B could be anywhere in the right circle. Therefore, the probability that sensor B exist in the highlighted area is shown in (3) where (1) and (2) values are substituted in (3).

The probability for sensor B to be in the highlighted area is 1 when sensors A and G have 0 distance. On the contrary, the probability is the least when sensors A and G have R distance in between.

$$\theta = \cos^{-1}\frac{D/2}{R} = \cos^{-1}\frac{D}{2R} \tag{1}$$

$$A_{AB} = 2\left(R^2\theta - \frac{D}{2}R\sin\theta\right) = 2R^2\theta - D \times R \times \sin\theta \tag{2}$$

$$P_{AB} = \frac{A_{XS}}{R^2\pi} = \frac{2\left(R^2\theta - \frac{D}{2}R\sin\theta\right)}{R^2\pi} = \frac{2\theta}{\pi} = \frac{2\sin\theta}{R\pi} \tag{3}$$

For the second stage of checking presented in Fig.5 given that G_1 is the one hop neighbor sensor for sensor A and the two hop neighbor sensor for sensor B, and G_2 is the one hop neighbor sensor for sensor B. Also, G_1 is distanced from G_2 within this range D ∈ [0,R] where R is the transmission range.

If both sensors A and B reside together either on the top highlighted areas or the bottom highlighted areas pin pointed by A_4. Then, A and B are not malicious.

$$A_4 = A_L - A_R \tag{4}$$

Given $A_L$that is the grey area of the left circle and A_R that is the grey area of the right circle, when they are subtracted we get the highlighted area A_4 that is calculated by (4) where A_L is calculated in (5) and A_R is calculated in (6).

$$A_L = \int_{-\frac{R}{2}}^{0} \sqrt{R^2} - \left(A + \frac{D}{2}\right)^2 dx$$

$$A_L = R\int_{-\frac{R}{2}}^{0} \sqrt{1 - \left(\frac{A + \frac{D}{2}}{R}\right)^2} dx$$

Given that $\frac{A+D/2}{R} = \sin t$, $dx = R\cos t\, dt$, $t = \sin^{-1}\frac{A+D/2}{R}$

$$A_L = R^2 \int_{\sin^{-1}\frac{-R+D}{2R}}^{\sin^{-1}\frac{D}{2R}} \sqrt{1 - \sin^2 t}\cos t\, dt$$

$$A_L = R^2 \int_{\sin^{-1}\frac{-R+D}{2R}}^{\sin^{-1}\frac{D}{2R}} \cos^2 t\, dt$$

$$A_L = \frac{R^2}{2}(t + \sin t\cos t)\int_{\sin^{-1}\frac{-R+D}{2R}}^{\sin^{-1}\frac{D}{2R}}$$

$$A_L = \frac{R^2}{2}\left[\sin^{-1}\frac{D}{2R} + \frac{D}{2R}\cos\left(\sin^{-1}\frac{D}{2R}\right) - \sin^{-1}\frac{-R+D}{2R} + \frac{-R+D}{2R}\cos\left(\sin^{-1}\frac{-R+D}{2R}\right)\right] \tag{5}$$

The upper A_4 areas are equal in size to the lower A_4 area.

$$A_R = \frac{R^2}{2}\left[\sin^{-1}\frac{-D}{2R} - \frac{D}{2R}\cos\left(\sin^{-1}\frac{-D}{2R}\right) - \sin^{-1} \times \frac{-R-D}{2R} - \frac{R+D}{2R}\cos\left(\sin^{-1}\frac{-R-D}{2R}\right)\right]. \tag{6}$$

The probability that sensor A and B is residing either in the upper A_4areas or the lower A_4 areas is presented in (8) that substitutes the results of (7) and (4).

$$A_A = A_B = R^2\pi - \left(2R^2\theta - D \times R \times \sin\theta\right) \tag{7}$$

$$P_{AB} = \frac{2A_4}{A_A + A_B} = \frac{2A_4}{2A_A} = \frac{A_4}{A_A} \tag{8}$$

Secondly, an analysis of the false positive based on the proposed method is presented in the following where this method aims on decreasing the false positive in sparse networks that have small number of sensors.

The false positive is addressed in sparse networks by having two checking stages because using the one hop neighborhood table alone in sparse networks increases the false positive since it may not find neighbors to build a neighborhood list. On the other hand, the two hop neighborhood list expand the area to search for neighbors.

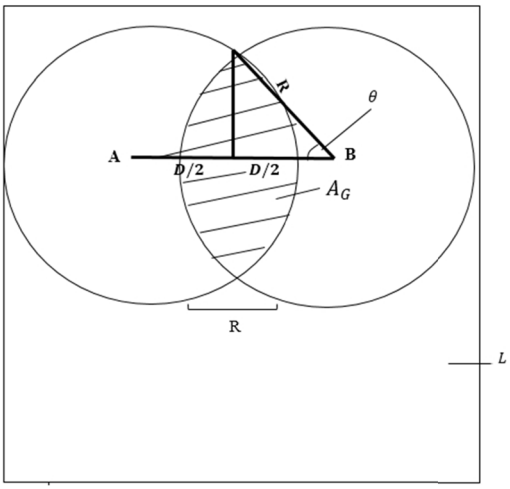

FIGURE 6. False positive for the proposed method.

In Fig. 6 Given L that is the network area where sensors are placed randomly. Moreover, A and B are two normal sensors that are not malicious and distanced from each other within this range D ∈ [0,R] where R is the transmission range.

For the first stage of checking, the probability of having a common neighbor for sensor A and B that exists on the highlighted area is presented in (10) with the use of (9). Unlike the second stage that has a higher probability value of having common neighbor presented in (11). Therefore, the second stage decreases the false positive in sparse networks.

$$A_G = 2R^2\theta - D \times R \times \sin\theta \tag{9}$$

$$P_{G1} = \frac{A_G}{L^2} \tag{10}$$

$$P_{G2} = P_{G1}^2 \tag{11}$$

C. THE SELECTED PROTOCOL

The proposed secured method is applicable on various routing protocols but in this work, it is applied for the Ad-hoc on-demand Distance Vector (AODV) routing protocol because it is one of the most popular routing protocols. It is categorized under reactive routing protocols that are known to be better than the proactive protocols as they consume less energy for transmission. It is less because it needs less periodic messages and sensors can sleep for longer duration of time. Furthermore, the memory usage is significantly decreased since it considers partial routes in the routing table. Nonetheless, it has a reduced overhead as the packets are not broadcasted periodically. Finally, it has power performance such that when routes are pruned suddenly it will be able to find alternative paths [25] and [26].

AODV protocol is categorized under on demand routing protocols where routing information are not stored permanently within the sensors but instead the routing path is searched for as the sensors need to send packets. It is described as when a sending sensor advertises a Route Request (RREQ) when it does not know the path to the destination and needs to know it. As a sensor receives a RREQ, it searches whether it has received a RREQ with the same sender IP address and RREQ ID in the last time for path discovery or not. If it was received earlier, the sensor quietly disposes the recent RREQ. If not, the sensor will forward the RREQ packet to search for the destination. As the RREQ is received by the destination it will generate the Route Reply (RREP) based on some principles and send it through the path that was used to discover the destination to reach the originator [27], [28], and [29]. The wormhole attack is powerful in AODV because it can forward RREQ packets through the generated tunnel directly to destination sensor. Therefore, the other RREQ packets originated by the source for the route discovery will be discarded. This will make other routes unable to be discovered which puts the attacker in a powerful position [30].

The proposed method starts as the RREP message is generated to be unicasted to the sender of this elected path in order to check the legitimacy before sending any data packets.

D. STRENGTHS AND LIMITATIONS

The main strengths of this method are that although the method is based on neighboring information, it solves the drawback of this technique as this method reduces the energy consumption since it does not force all discovered routes to be tested. The elected route is only tested where sensor nodes in the elected path and their one hop neighbors are responsible to perform the calculations. In addition, it does not expand the span of the network traffic and acquires an insignificant transmission capacity overhead, adding a minimal effort to the system for improving its level of security. Also, it does not need additional hardware e.g., GPS or synchronized clocks. In addition, it is based on simple computations and therefore, no increase in the delay or energy consumption. Moreover, the property of finding intersection of the second-degree neighbors decreases the false positive in sparse networks. Furthermore, it has a very high detection rate of 100 % for tunnels of four hops or more in length because sensor A builds one hop neighborhood list and sensor B builds two hop neighborhood list and therefore sensor A and B can search for alternative path between them that is of length of three hops. So, if the generated malicious tunnel is of four hop in length, then sensor A and B would not be able to search for this generated malicious path.

On the other hand, the limitations of this method are the two malicious sensors could fabricate their neighborhood list to manipulate the detection method. In addition, usually it is very rare to detect this attack if the tunnel is shorter than four hops.

IV. EXPERIMENTAL SETUP AND RESULT EVALUATION

Table 1 indicates the simulation parameters where sensors have a random location that is generated when the file is run for the first time. These sensors locations are stored in a text file to read those locations in further runs. This is

TABLE 1. Network simulation parameters.

Parameter	Value
Network area	100m x 100m
Network size	50, 90, 150
Sensors position	Random
Transmission range	20 meters
Transmission range for wormhole nodes	As long as the tunnel
Mobility	static
Routing protocol	AODV
Simulation time	150 seconds
Packet size	500 bytes

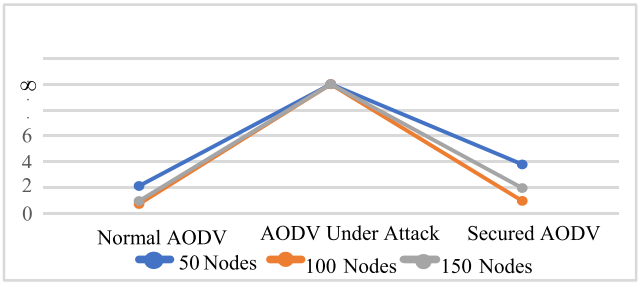

FIGURE 7. End to end delay.

done to have constant positions for all implemented files. In other words, network topology must be the same for the normal network implementation, the network under attack implementation, and the secured network implementation to have a fair comparison. The transmitted information is a text file of size 2842 bytes. It is divided into chunks of 500 bytes then placed in a buffer. Then, generate packets from that buffer, send them and then at the destination read the buffer and append the content to a buffer to reconstruct the original file.

In this work a discrete event simulator for networks is used, called network simulator (NS3). The used version in this work is version 3.28. The NS3 is mainly used for research and educational purpose. The NS3 simulator is equipped with the NetAnim animator that is used to show visualization.

In Fig. 7 and 8 the x-axis shows the three network scenarios and the y-axis shows the corresponding values for different results parameters. They present the secured method evaluation when the malicious sensors are detected in the network. This is when the wormhole tunnel is of four hops or more in length but when having a wormhole tunnel of a less length it might not detect the malicious sensors and therefore have a performance similar to the malicious scenario.

Fig. 7 presents the delay value that is identified by the time required to deliver the complete file and since malicious sensors drop packets, it will never be delivered completely. Therefore, an infinity value is used for the attack case because it will never deliver the message. It is very clear that the

TABLE 2. Throughput results.

	Normal AODV	AODV Under Attack	Secured AODV
50 Nodes	14481.5	0	14422.3
100 Nodes	41136.8	0	39712.8
150 Nodes	36969	0	36409

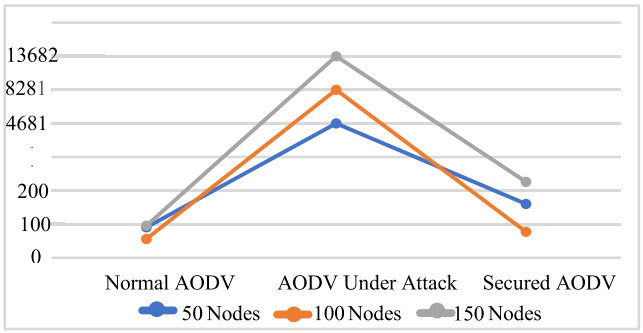

FIGURE 8. Energy consumption.

proposed secured method has small increase in the delay value that is hard to be mentioned. The added delay for the detection method in the 50-node network size is 1.7 second. In addition, in the 90-node network size the added delay for transmission is 0.2 second. Furthermore, the 150-node network size an additional 1 second used for detection. The amount of delay required to perform the proposed security measure is positively correlated to the length of wormhole tunnel and the neighborhood lists size. In Fig. 7 the end to end delay has the highest values for the 50-nodes network size, and the reason for that is presented in Fig. 9 were the tunnel is longer than networks of size 100-nodes and 150-nodes that are presented in Fig. 10 and 11.

The Throughput is identified by the number of bits transmitted per second. In Table 2 the network under attack has a zero value for the throughput and that is due malicious nodes are dropping all packets and therefore no further packets exist in the path. In addition, the secured method has a value that is very close to the normal value.

Table 2 describes the throughput values where the 50-nodes network size has the smallest decrease in the throughput value. The reason behind that is the calculation of throughput that is by dividing the complete transmitted message over the delay time and since the transmitted message is constant in size, it is affected only by the delay value. Therefore, and since the 50-nodes network size has the highest delay value, it has the least decrease in the throughput.

The method is energy preserving as shown in Fig. 8 where the average additional energy in 50-nodes network size was 70 Joules, and the average additional consumed energy in 90-nodes network size was 21 Joules, and in the case of 150-nodes network size the additional energy was 129 Joules.

The amount of energy consumption required to perform the proposed security measure is positively correlated to the

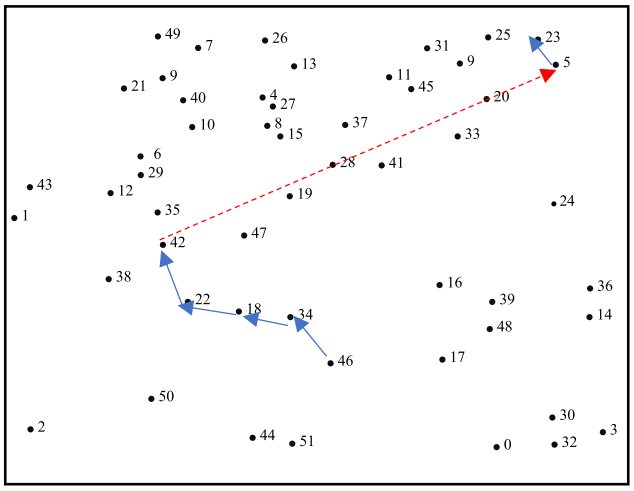

FIGURE 9. Network under attack with 50 nodes and two malicious nodes 42 and 5.

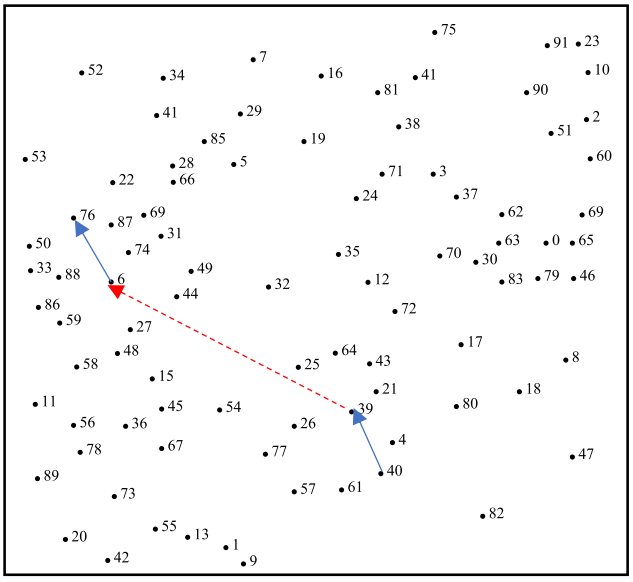

FIGURE 10. Network under attack with 90 nodes topology and two malicious nodes 39 and 6.

length of wormhole tunnel and the neighborhood lists size. Furthermore, energy consumption is the highest in 150-nodes network because it has a very dense neighborhood table.

The 100-nodes network size has the least values for energy and end to delay because compared to the 50-nodes network size it has a shorter tunnel and compared to the 150-nodes network size it has a smaller neighborhood lists were node-76 has {53,86,87,50,88,74,31,69,22,33,6}neighbors, node-6 has{86,48,87,76,69,59,88,50,49,33,27,74,58,31,44} neighbors, and node-39 has {40,4,57,77,64,21,26,25,61,43} neighbors.

The 150-node network size has a greater value than the 100-nodes network size in energy and end to end delay because in is denser therefore, has a longer neighborhood list were node-79 has {1, 57, 87, 140, 89, 53, 88, 63, 149, 80, 59, 25} neighbors, node-59 has {1, 57, 87, 140, 89, 53, 12, 149,

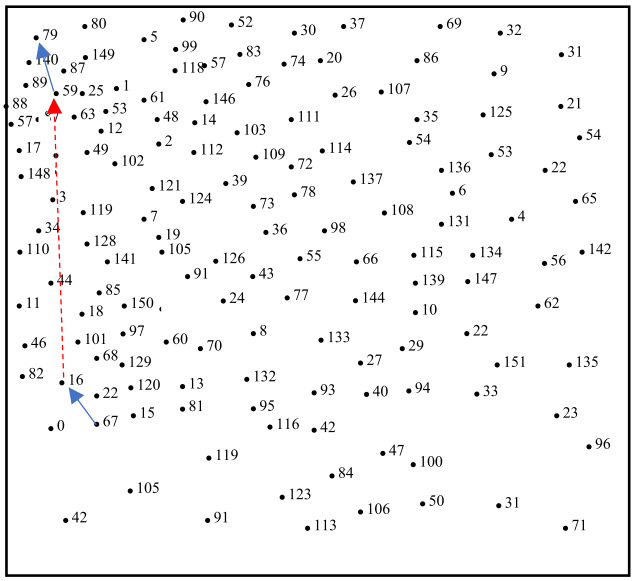

FIGURE 11. Network under attack with 150 nodes topology and two malicious nodes 16 and 59.

25, 88, 63, 61, 102, 17, 3, 2, 49, 79, 48, 148, 80, 5} neighbors, and node-16 has {67, 0, 101, 82, 81, 68, 97, 15, 22, 13, 120, 60, 46, 18,129} neighbors.

Moreover, the packet delivery ratio is identified by the successfully delivered packets to destination and once the malicious nodes are detected the secured method uses an alternative path for transmission and therefore the secured measure can deliver the complete message by this alternative path.

Energy consumption is rarely addressed in existing techniques but in [11], and [18] it was mentioned. In [11] the secured method has dropped the energy consumption to 50% compared to the network under attack. Moreover, in [18] the aim was to propose an Energy Efficient Intrusion Detection System by lowering the energy consumption where it was reduced by 8% compared to other existing intrusion detection systems in the AODV routing protocol. However, our proposed secured method has dropped energy consumption to 95%, 96%, and 97.5% compared to networks under attack for 50-nodes, 100-nodes and 150-nodes network sizes respectively.

V. CONCLUSION

Wireless Sensor Networks are made of sensors that has the capability of sensing their surroundings environment to deliver the information to a base station that has a connection to the Internet. It is an important filed because it has a major role in wide applications as it serves surveillance, health, traffic and much more. It is spatially distributed hence it must have low cost because of that sensors have limited batteries, computational ability and memory size. Therefore, its restrained ability to implement common security measures makes it vulnerable to various types of attacks. There are

various types of attacks targeting different network layers. One type is wormhole attack that is a harmful and easily deployed attack that targets the routing layer. Wormhole attack is described as generating untrusted shortcut through the network. This is formed when two intruder sensors establish a wired or wireless connection between them.

This paper proposes an energy preserving method to detect this attack. The method is applied on the AODV protocol. The method has two stages that is applied for all sensors in the elected path of transmission. Passing a stage relieves the protocol from checking the later stage. Both stages are based on connectivity and neighborhood information. If none of these stages are fulfilled, then a wormhole is detected and a blacklist having the identity of these malicious sensors is broadcasted.

This method has achieved a very high detection accuracy of 100% for wormhole tunnels of four hops in length and has no additional equipment. Moreover, it is efficient in terms of energy, throughput, packet delivery ratio, and end to end delay.

REFERENCES

[1] Z. Qian and Y.-J. Wang, "Internet of Things-oriented wireless sensor networks review," *J. Electron. Inf. Technol.*, vol. 35, no. 1, pp. 215–227, 2014.

[2] C. Guy, "Wireless sensor networks," in *Proc. 6th Int. Symp. Instrum. Control Technol., Signal Anal., Meas. Theory, Photo-Electron. Technol., Artif. Intell.*, Nov. 2006, Art. no. 63571I.

[3] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[4] G. Serpen, J. Li, and L. Liu, "AI-WSN: Adaptive and intelligent wireless sensor network," *Procedia Comput. Sci.*, vol. 20, pp. 406–413, Jan. 2013.

[5] I. Tomić and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet Things J.*, vol. IOT-4, no. 6, pp. 1910–1923, Dec. 2017.

[6] S. Bhagat and T. Panse, "A review on detection and prevention of wormhole attack in wireless sensor network," *Int. J. Comput. Appl.*, vol. 127, no. 13, pp. 1–4, Oct. 2015.

[7] A. S. K. Pathan, H.-W. Lee, and C. S. Hong, "Security in wireless sensor networks: Issues and challenges," in *Proc. 8th Int. Conf. Adv. Commun. Technol.*, Feb. 2006, p. 6.

[8] G. Farjamnia, Y. Gasimov, and C. Kazimov, "Review of the techniques against the wormhole attacks on wireless sensor networks," *Wireless Pers. Commun.*, vol. 105, no. 4, pp. 1561–1584, Apr. 2019.

[9] 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.

[10] L. Ahmed, S. Larbi, and K. Bouabdellah, "A security scheme against wormhole attack in MAC layer for delay sensitive wireless sensor networks," *Int. J. Inf. Technol. Comput. Sci.*, vol. 12, pp. 1–10, Nov. 2014.

[11] P. Amish and V. B. Vaghela, "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol," *Procedia Comput. Sci.*, vol. 79, pp. 700–707, Jan. 2016.

[12] T. Minohara and K. Nishiyama, "Poster: Detection of wormhole attack on wireless sensor networks in duty-cycling operation," in *Proc. Int. Conf. Embedded Wireless Syst. Netw.*, Feb. 2016, pp. 281–282.

[13] M. Imran, F. A. Khan, T. Jamal, and M. H. Durad, "Analysis of detection features for wormhole attacks in MANETs," *Procedia Comput. Sci.*, vol. 56, pp. 384–390, Jan. 2015.

[14] A. P. Rai, V. Srivastava, and R. Bhatia, "Wormhole attack detection in mobile ad hoc networks," *Int. J. Eng. Innov. Technol.*, vol. 2, pp. 174–179, Aug. 2012.

[15] K. Patidar and V. Dubey, "Modification in routing mechanism of AODV for defending blackhole and wormhole attacks," in *Proc. Conf. IT Bus., Ind. Government (CSIBIG)*, Mar. 2014, pp. 1–6.

[16] M. Sookhak, A. Akhundzada, A. Sookhak, M. Eslaminejad, A. Gani, M. K. Khan, X. Li, and X. Wang, "Geographic wormhole detection in wireless sensor networks," *PLoS one*, vol. 10, no. 1, 2015, Art. no. e0115324.

[17] H. Chen, W. Chen, Z. Wang, Z. Wang, and Y. Li, "Mobile beacon based wormhole attackers detection and positioning in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 3, 2014, Art. no. 910242.

[18] G. Jegan and P. Samundiswary, "Wormhole attack detection in zigbee wireless sensor networks using intrusion detection system," *Indian J. Sci. Technol.*, vol. 9, no. 45, pp. 1–10, 2016.

[19] K.-F. Krentz and G. Wunder, "6lowpan security: Avoiding hidden wormholes using channel reciprocity," in *Proc. 4th Int. Workshop Trustworthy Embedded Devices*, Nov. 2014, pp. 13–22.

[20] N. Labraoui, M. Gueroui, and M. Aliouat, "Secure DV-Hop localization scheme against wormhole attacks in wireless sensor networks," *Trans. Emerg. Telecommun. Technol.*, vol. 23, no. 4, pp. 303–316, Jun. 2012.

[21] X. Lu, D. Dong, and X. Liao, "MDS-based wormhole detection using local topology in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 8, no. 12, pp. 1–9, 2012.

[22] Q. Shen, Z. Zhao, W. Niu, Y. Liu, and H. Tang, "Tolerance-based adaptive online outlier detection for Internet of Things," in *Proc. IEEE/ACM Int. Conf. Green Comput. Commun. Int. Conf. Cyber, Phys. Social Comput.*, Dec. 2010, pp. 560–565.

[23] T. Bin, Q. Li, Y.-X. Yang, D. Li, and Y. Xin, "A ranging based scheme for detecting the wormhole attack in wireless sensor networks," *J. China Universities Posts Telecommun.*, vol. 19, pp. 6–10, Jun. 2012.

[24] S. Song, H. Wu, and B.-Y. Choi, "Statistical wormhole detection for mobile sensor networks," in *Proc. 4th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2012, pp. 322–327.

[25] K. Thangaraj and T. Selvi, "Comparative study of proactive, reactive and hierarchical routing protocols," *i-Manager's J. Wireless Commun. Netw.*, vol. 3, pp. 1–6, Oct./Dec. 2014.

[26] I. M. A. Fahmy, L. Nassef, and H. A. Hefny, "Energy consumption efficiency and performance evaluation of DSDV and AODV routing protocols," *Int. J. Comput. Netw. Wireless Commun.*, vol. 4, no. 2, pp. 113–118, 2014.

[27] Y. J. Zhu, Y. Q. Li, Q. G. Fan, and Z. Wang, "Ad hoc on-demand distance vector routing protocol based on load balance," in *Proc. MATEC Web Conf.*, 2016, Art. no. 02090.

[28] V. Kumar and A. Kush, "Worm secure protocol for wormhole protection in AODV routing protocol," *Int. J. Comput. Appl.*, vol. 44, pp. 15–21, Apr. 2012.

[29] H. Simaremare, A. Abouaissa, R. F. Sari, and P. Lorenz, "Security and performance enhancement of AODV routing protocol," *Int. J. Commun. Syst.*, vol. 28, no. 14, pp. 2003–2019, 2015.

[30] R. Ahuja, A. B. Ahuja, and P. Ahuja, "Performance evaluation and comparison of AODV and DSR routing protocols in MANETs under wormhole attack," in *Proc. IEEE 2nd Int. Conf. Image Inf. Process. (ICIIP)*, Dec. 2013, pp. 699–702.

WATEEN A. ALIADY received the B.S. degree in computer science from Princess Nourah Bint Abdulrahman University and the M.S. degree in computer science from King Saud University, Riyadh, Saudi Arabia.

SAAD A. AL-AHMADI is currently an Assistant Professor of computer science with the College of Computer and Information Sciences, King Saud University. He has published many papers in many journals and conferences. His research interests include cybersecurity, computer networks, mobile ad hoc networks, and sensors networks.