Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 4853924, 19 pages
http://dx.doi.org/10.1155/2016/4853924

Research Article

Analysis of Denial of Service Impact on Data Routing in Mobile eHealth Wireless Mesh Network

Shaker Alanazi,[1,2] Kashif Saleem,[1] Jalal Al-Muhtadi,[2] and Abdelouahid Derhab[1]

[1]*Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh 12372, Saudi Arabia*
[2]*College of Computer & Information Sciences, King Saud University, Riyadh 12372, Saudi Arabia*

Correspondence should be addressed to Kashif Saleem; ksaleem@ksu.edu.sa

Received 12 January 2016; Accepted 8 June 2016

Academic Editor: Laurence T. Yang

Wireless mesh networks (WMNs) are a promising technology that has emerged with the combination of several wireless networks. These wireless networks and devices communicate in a mesh network manner, to provide edge-to-edge, easy, and cost-effective data communication. Many current and future promising applications depend on WMN and one of the most important applications is eHealthcare, where the confidential information transfers with the help of WMN. WMN devices communicate over a wireless medium, which opens the system to a number of vulnerabilities; thus, an intruder can launch malicious activities through many types of attacks that can result in denial of service (DoS). In this paper, the available solutions to overcome these attacks are simulated and evaluated in terms of data packet delivery ratio, end-to-end delay, and network throughput and under different cases of static and mobile WMNs, which helps in providing suggestions to enhance existing protocols and mitigate the effect of DoS caused by such attacks.

1. Introduction

Security is always a major concern in transferring information from the source to the destination, whether it is the manual postal service or data communication in today's digitized world, especially, applications like eHealthcare that are built to provide assistance for a very sensitive purpose. Over the years, many communication technologies have been introduced and numerous protocols have been proposed to handle security issues. One promising and growing wireless communication technology is the wireless mesh network (WMN). In eHealthcare, WMN plays a very important role in transferring confidential information hop by hop until the required destination. A WMN is a self-organized and self-configured network, where nodes and networks communicate in a mesh network manner to provide connectivity [1]. A WMN consists of nodes that communicate using wireless technology to provide connectivity. These nodes are usually mesh clients such as cell phones and mesh routers, including Wi-Fi access points. A WMN has a decentralized architecture where mesh clients and routers communicate in a distributed manner to provide the connection [2]. The authors of [3] discussed the main design factors that affect the architecture of a WMN and the selected components to build the WMN, such as signal transmission techniques, scalability, connectivity, the quality of broadband services, security, ease of use, and compatibility. WMN nodes can be connected and organized in three main ways to form three types of WMNs: infrastructure/backbone, client, and hybrid WMNs. The main characteristics and benefits of WMNs are coverage, mobility, scalability, heterogeneity, and compatibility [3] and provide network services such as Internet access, video conferencing, and voice communication, and they help in transferring data between networks. This makes a WMN suitable for many applications in both military and civilian fields. Public safety and disaster recovery (PSDR) wireless communication systems are an example where a WMN is strongly applicable [3, 4]. In such applications, wired communication may not be possible or risky, so a WMN is a more suitable solution because it offers easy and rapid connectivity through a wireless medium.

A WMN can be seen as a group of nodes (clients or routers) that cooperate to provide connectivity. Such an open architecture, where clients serve as routers to forward

data packets, is exposed to many types of attacks that can interrupt the whole network and cause denial of service (DoS). Moreover, the mobility factor in the network makes the security of the network more difficult and challenging. For this reason, protection against DoS problems is essential and requires secure routing protocols. These secure routing protocols must detect, identify, and isolate attacks that can cause DoS, and they must keep the routing functionality working.

Very common and serious attacks on WMN routing that can lead to DoS are selective forwarding, hello flooding, and wormhole attacks [17, 18]. In a selective forwarding attack, the packets that pass through malicious nodes are routed by these nodes inconsistently to distribute the network. In a hello flooding attack, a malicious node transmits hello messages with high transmission power to convince the remaining nodes that it is a neighbor to many nodes in the network. A wormhole attack is one of the most dangerous attacks in a WMN network layer. In this type of attack, a malicious node tunnels messages from one part of the network to another part and replays them. To make the situation worse, a high-speed link with low latency is usually used to tunnel these messages, which makes the link more tempting to be selected in the routing protocols. All of these types of attacks aim to disrupt the routing process to cause the DoS problem. A selective forwarding attack tries to cause DoS directly by dropping some of the routed packets. In contrast, in hello flooding and wormhole attacks malicious nodes try to give themselves a greater chance of being selected by the routing protocol as a routing path; then they can perform any activity to distribute the network and introduce DoS.

Even though the WMN is a promising technology, it faces many challenges, some of which are mentioned above. This paper studies the impact of three recent and common types of attacks on mobile WMNs: selective forwarding, wormhole, and hello flooding attacks. Moreover, this paper will study existing solutions to overcome these attacks on the mobile environment. A part of this work was presented previously in [19] as a preliminary report.

To achieve the objective, the three types of attacks are simulated using OMNET++ on Ad hoc On-Demand Distance Vector Routing (AODV). AODV was selected because it is proposed as a possible routing protocol in IEEE 802.11s [20]. Moreover, AODV is available in many simulation tools, including OMNET++. The attacks are simulated on the OADV routing protocol in two modes. In the first mode, malicious nodes are stationary, and, in the second mode, the network contains mobile malicious nodes. In both modes, the impact of the attacks on the packet delivery ratio, end-to-end delay, network throughput, and energy consumption are measured. This will highlight the impact of these attacks on the network, as well as the effect of mobility on increasing or decreasing the damage caused by the attacks.

After studying the impact of the attacks on stationary and mobile networks, the study will concentrate on the available solutions discussed in the literature to overcome the attacks. More specifically, the same simulations and experiments performed on AODV will be conducted on a security protocol called Position-Aware, Secure, and Efficient Mesh Routing (PASER). This will measure PASER's immunity to the three types of attacks on both stationary and mobile networks. The research will contribute to the field as follows:

(i) Implementing 28 scenarios that include AODV and the WMN protocol PASER in OMNET++ for both malicious and legitimate scenarios.

(ii) Evaluating the AODV and PASER protocols by incorporating selective forwarding, wormhole, and hello flooding attacks in a mobile WMN; to the best of our knowledge, this study is the first of its kind.

(iii) Evaluating and measuring the effectiveness of the two principle protection mechanisms, cryptography and a GPS module, against attacks in a mobile network.

(iv) Providing suggestions that facilitate future research studies to simulate different WMN scenarios and the adoption of appropriate security mechanisms.

This paper is structured as follows. Section 2 discusses the issues and challenges faced by WMNs, reviews the related and recent literature, and gives comparison of the available solutions. Section 3 presents implementation and results of attacks on AODV and PASER. Section 4 exhibits the discussion and recommendations. The conclusion and future work are provided in Section 5.

2. Literature Review

The routing layer in a WMN, where packets travel from the source to the destination in a multihop manner, is one of the main differentiators of a WMN from other types of networks. Such a mechanism makes a WMN more vulnerable to network attacks, such as black holes, wormholes, grey holes, and packet dropping. Although many secure routing protocols have been proposed to address the security vulnerabilities, there is still significant room to enhance the security and usability of WMN secure routing protocols. In this section, the current state-of-the-art secure routing protocols are reviewed.

2.1. Issues and Challenges Faced by WMNs. A wireless mesh network (WMN) is a type of network where nodes cooperate and transfer data packets hop by hop. In hop-by-hop communication, network security is the responsibility of not only the routers but also each node in the network. When regular nodes contribute to communication over the wireless medium, they are vulnerable to many types of attacks that can lead to a denial of services (DoS) in the WMN. Moreover, when mobile nodes are joining or leaving the WMN, the problem becomes more complicated because a trust issue can arise between the mobile nodes and the network.

Still, there are open challenges and issues in WMNs to be addressed by the research community and industry, as these challenges affect the usability of WMN technology in most applications. In [1], the authors discuss the open issues and challenges of WMNs at every layer. One of these open issues in the routing layer is the need for a protocol that is efficient specifically for WMNs. As described in [1], efficient

routing protocols are distributed and independent of any traffic profile, and they feature link quality variation and minimum overhead.

Some of the most important challenges faced by WMNs are network provisioning and network integration. In network provisioning, there is a need for a sophisticated management tool to enable mesh routers and mesh clients to dynamically establish connections and to manage the mobile nodes. Since a WMN contains various types of technologies and protocols, it is necessary to have standard mechanisms to integrate these technologies. For example, some mesh routers are based on IEEE 802.11, while others are based on different standards, such as IEEE 802.15.4 and IEEE 802.16.

Security is one of the most important issues that need to be addressed in WMNs. Unfortunately, WMNs are vulnerable to multiple types of attacks because of their special characteristics, such as their ad hoc nature and use of a wireless medium to communicate [4].

In the physical layer, WMNs are vulnerable to jamming attacks, according to [17], for example, trivial signal jamming where the attacker transmits a noise signal to disrupt the WMN radio signal. In addition, a WMN's physical layer is vulnerable to reactive jamming, where the attacker transmits noise whenever it detects that a legitimate node has started to use the channel. Moreover, in some applications of WMNs, the installation or usage environment is not secure, such as in remote areas, which gives attackers the ability to tamper with the system to extract important information or even destroy the units.

The MAC layer in a WMN is vulnerable to many types of attacks. Some examples provided in [17] are jamming attacks and MAC spoofing. In jamming attacks, an attacker can try to disrupt the communication channel by sending complete MAC frames. An unprompted Clear-to-Send (CTS) attack, a reactive Request to Send (RTS), and corrupt jamming (CJ) are some examples of possible MAC jamming attacks in a WMN's MAC layer.

The network layer of a WMN is also vulnerable to multiple types of attacks that may lead to the DoS problem. In [17], examples of attacks are given that can target the network layer in the control or data plan. In the control plan, rushing, routing table overflow, Sybil, wormhole, and sinkhole attacks are some examples. The most basic data plan attack is eavesdropping, where a malicious node tries to learn the network topology by listing to the traffic.

Many types of attacks can be launched in the transport and application layers of a WMN. In the transport layer, an attacker can try to flood the network by repeatedly issuing connection requests to a specific resource in the network [17]. The application layer is also vulnerable to many types of attacks, including viruses, worms, and malicious codes and application abuse [17].

A great deal of effort has been put into treating WMN security issues and proposing suitable solutions at many levels and in various applications. For example, in [18, 21], the authors study the security requirements and the impact of implementing security measures in WMNs in general, while, in [22], the performance of the routing protocol of an 802.11-based WMN under attack is studied. Many solutions have been proposed to handle WMN security requirements, either to solve a specific challenge, such as the key establishment mechanism proposed in [23], or by providing a more comprehensive solution, as discussed in the next section. The next section discusses recent security solutions and secure routing protocols developed to protect the WMN network layer, mainly against attacks that can lead to DoS.

2.2. Recent Related Work. The authors in [5] propose a routing protocol to protect WMNs against wormhole attacks called "wormhole-resistant secure routing for wireless mesh network (WRSR)." The authors of the paper followed a new approach that aims to detect the presence of wormhole nodes and links and quarantine them before using the links. WRSR depends on the neighbors' information and the existence of alternative subpaths to detect the existence of a wormhole. WRSR uses statistical probability to categorize the paths as either safe, "wormhole free," or unsafe, "containing a wormhole." In the proposed protocol, WRSR represents the transmission range of a node and d is the distance between two nodes. The authors use a unit disk graph to prove that the probability of finding an alternative path where $R < d < 2R$ is high, and any path that does not fit in this category is considered insecure. To implement the protocol, IEEE 802.11s frames are extended to contain the necessary information to make WRSR work, which are a flag bit to indicate the existence of neighboring information and the neighboring addresses to accommodate various neighbors' numbers. To simulate and test the proposed protocol, a strong adversary model is used where malicious nodes can establish links with high speed and low latency. Moreover, the attacker can compromise mesh routers in the network to lunch attacks. In the simulation, the protocol shows a very high correct rate of detection of wormhole links when the network is dense and contains many alternative subpaths.

In [6] the authors have proposed an efficient and secure routing protocol for a hybrid wireless mesh network (WSRPHWM) that depends heavily on public cryptography to secure routing. First, it is important to mention that WSRPHWM is based on a route-on-demand protocol called the cross-layer secure and resource-aware on-demand routing protocol (CSROR), where WSRPHWM inherits the routing metrics used in CSROR. The routing metrics used depend on three factors to quantify routes: the available bandwidth, node battery power, and unreliability level. The unreliability level is based on value assigned by a node's neighbor to indicate the past experience of forwarding packets on a particular route. To maintain security, WSRPHWM uses symmetric key cryptography, asymmetric key cryptography, and the MAC function to authenticate and encrypt routing data. WSRPHWM assumes that the network has a certification authority (CA) that issues and signs certificates for each node and router in the network. The first step taken by each node is to establish a secure session using the Diffie-Hellman elliptic curve with each of its neighbors to generate a trusted session key between them. After that, for each message that includes a route request, the sender node encrypts the mutable fields of the request using the session keys for each neighbor, signs the nonmutable fields using its private key, and finally generates

a MAC using the mutual session key. For each neighbor, the process is repeated. When the neighbor receives the request, it first validates the MAC and the signature of the packet and then decrypts the mutable fields to alter them. After that, it repeats the process done by the source node and then forwards the request to its neighbors. When WSRPHWM is compared with other protocols, such as SADOV and CSROR, it shows very good results with respect to the average end-to-end delay and routing overhead. For the average end-to-end delay, WSRPHWM shows better performance than SADOV, but the delay is longer than that of CSROR because it uses the crypto operations. WSRPHWM causes the smallest routing overhead among the three protocols.

The cross-layer secure and resources-aware on-demand routing protocol (CSROR) for hybrid wireless mesh networks proposed in [7] uses the history of communication to decide which route is trustworthy. To do so, the route selection parameters include a threat level (TL) field in addition to the power level and available bandwidth. The TL of the route is the sum of the drop values (DV) of nodes in the route, while the DV of each node is the percentage of unacknowledged messages. In CSROR, each node keeps the drop value of each of its close neighbors (one level). The DV is calculated by subtracting the number of packets passively acknowledged by the direct neighbor of the current node neighbor. When the route discovery process starts in CSROR, the source node broadcast route request packet (RREQ) and the destination select the best route according to the aforementioned parameters. CSROR shows better results than AODV and ASODV in terms of efficiency and reliability, particularly in the packet delivery rate and average delay.

In [8], the authors propose a routing scheme based on the ADOV distance vector algorithm to provide secure routing, using different control packets for routing requests and routing request replies. The selection of the route in the proposed routing protocol is based on two factors: the data rate and node reputation value (RV). The selection of the route is done by the destination when it receives routing request packets. The route that has the highest reputation and the lowest data rate is selected. The RV of each node is generated by its neighbors to signify previous successful communication, and the available data rate is calculated by exchanging information between the network and the MAC layer.

Authenticated Routing for Ad hoc Networks (ARAN) in [9] is another routing protocol that depends heavily on cryptography to provide security. ARAN requires the existence of a certificate server responsible for issuing, distributing, and revoking certificates. In ARAN, each node must have a certificate signed by and trusted by this server to be considered trusted. The certificate of each node must contain the IP address, its public key, a time stamp to indicate when the certificate was created, and the expiry date. In the route discovery process, the source signs a route request packet (RREQ) and broadcasts it to its neighbors. The neighbors first validate the packets and then sign and broadcast them. When the destination receives the request packet (RREQ), it sends a reply using the reverse path. Moreover, it signs the reply and includes its certificate in the reply, and the same sequence of signing and verifying that took place in the route discovery is repeated until the reply reaches the source. Finally, when a certificate is to be revoked, the trusted server will broadcast a signed request for the certificate to be revoked. Each node rebroadcasts the request to its neighbors.

The SAODV protocol proposed in [10] aims to secure AODV using cryptography. In fact, it solves many security flaws in AODV. The first flaw is the possibility for an attacker to impersonate an S node by forging route request packets (RREQ) using its address as the source address. The second security flaw is that the hop counts in RREQ packets are reduced to select the best route. The third flaw is the ability to impersonate a destination node by replying to RREQ as if it is the destination. To solve these security issues, SAODV uses cryptography, mainly hashing and digital signatures. SAODV assumes the existence of a key management system that is responsible for issuing nodes' keys and revoking them if needed. It is important here to mention that these keys or certificates must associate the key with the address of the nodes, which is a challenge because of the dynamic nature of WMN networks. Once all nodes have their public keys or certificates, they can start communication. In ADOV, the RREQ hop count is the only mutable field that can be secured using a hashing chain. The nonmutable fields in RREQ and RREP can be secured using a digital signature.

A modified version of Secure Efficient Ad hoc Distance (I-SEAD) vector routing is proposed in [11] based on the destination sequenced distance vector (DSDV) with the enhancement of adding security to the routing. I-SEAD uses a one-way hash chain to authenticate the routing update. To build the one-way hash chain, I-SEAD uses a cryptographic hash function; the one-way hash chain is computed by conducting consecutive hashing, $h_i = H(h_{i-1})$ for $0 < i \leq n$, for some n and when the first value in the chain, x, is randomly generated for each node. This process enables nodes to determine whether the updates came from a legitimate node. I-SEAD assumes the existence of trusted distribution authority to distribute the initial values of nodes.

In [12], the Security-Aware Ad hoc Routing (SAR) for wireless networks is discussed. SAR includes security as a parameter in the route discovery process. Moreover, it provides a security framework that can be adapted by any application that uses SAR according to the required level of security. SAR protects the route discovery process by allowing only nodes that have at least the same level of security to contribute to the process. The required level of trust is embedded in the route request packet (RREQ); nodes that cannot satisfy the required level of security cannot forward or reply to the route request. Moreover, SAR uses cryptography to provide message authentication, message integrity, message confidentiality, and node authentication.

In [13], the designers propose a new methodology to detect malicious routing activity by colluding nodes in WMNs. The new methodology is not an independent and complete secure routing solution; it is a mechanism to be integrated into routing protocols to detect malicious routing activities. The proposed solution, called Leak Detector, is based on graph theory, where the destination node of the route builds a virtual graph to model the paths from the

source to the destination. Using this virtual graph, the destination node calculates the ratio of the incoming and outgoing traffic for each intermediate node in the path and uses this information to decide whether an intermediate node is malicious or not. When the deviation between the incoming traffic and outgoing traffic is high, this node is considered malicious. The proposed mechanism detects only selective forwarding or the complete dropping of packets, and it assumes the existence of multiple paths from the source to the destination.

A secure routing protocol against wormhole attacks in a sensor network (SeRWA) is described in [14]. SeRWA uses neighbor information to detect wormholes. In terms of security, SeRWA provides a way to detect wormholes and provides authentication between neighbors using a pair-wise key. To detect wormhole tunnel, each node builds a list of its neighbors and shares this list with all its neighbors. When a neighboring node exists in the node's routing table and does not exist in its routing table of neighbors, the protocol uses the distance between these neighbor nodes and transmission power to decide whether the missing node is part of a wormhole tunnel. A simulation of SeRWA is performed using NS2 and shows a low rate of false positive detection of less than 10%.

In [15], the authors propose a secure routing protocol against routing disruption in MANET networks called CRP. The proposed protocol is based on dynamic source routing (DSR) and uses public key cryptography to detect tampering with packets or fake packets. The proposed protocol assumes the existence of monitoring nodes to monitor intermediate nodes between monitoring nodes and collect statistics about the routing behavior of these nodes to detect black hole and grey hole attacks. The proposed protocol is simulated using NS2 and compared to the DSR protocol. For a black hole attack in which malicious nodes form about 40% of the network, CRP achieves a more than 70% packet delivery rate, while DSR achieves less than 50%. For a grey hole attack, CRP achieves about an 80% packet delivery rate and DSR achieves about 70% when 30% of the network nodes are malicious.

2.2.1. Position-Aware, Secure, and Efficient Mesh Routing (PASER). In [16], the authors propose a routing protocol called Position-Aware, Secure, and Efficient Routing (PASER) discovery protocol for wireless mesh networks. PASER is a reactive routing protocol that uses cryptographic operations to protect the routing of packets in mesh networks. The designers of PASER stated three main goals to be accomplished by PASER.

(i) *Protection against External Attacks.* PASER uses public key cryptography to identify nodes and give the nodes the ability to take part in the routing mechanism. This is accomplished by the existence of a key distribution center (KDC) that issues certificates for trusted nodes. This can be compromised only by compromising the session keys or node certificates.

(ii) *Isolate and Exclude Malicious Nodes from the Network.* Even though this is one of objectives of PASER, the designers did not implement a specific mechanism to accomplish this; instead, this is done by the route discovery process. The designers of PASER discussed a variety of options that can be implemented, including the adoption of a honeypot.

(iii) *Reducing the Impact of Malicious Nodes in the Network.* This objective is accomplished by using cryptographic functions to limit the operations that can be performed by malicious nodes in the routing process. For example, message authentication is used to prevent malicious nodes from faking or altering messages. Message freshness is also used to prevent the replaying of old messages. Moreover, origin authentication is implemented by PASER to verify the origin of a message. One important protection mechanism in the routing process is neighbor authentication to ensure that the neighbor is in transmission range, which is the main defense mechanism against wormhole attacks. This is done in PASER by associating the digital signature of the neighbor with the neighbor's GPS location.

There is an existing implementation of the complete protocol that can be integrated to OMNET++, where OpenSSL is used as the encryption library.

2.2.2. Ad Hoc On-Demand Distance Vector Routing (AODV). According to AODV RFC 3561 in [24], AODV is a reactive routing protocol that establishes the route only when there is data to be sent. AODV has three main advantages that make it attractive to be used in WMNs:

(i) It is loop-free.

(ii) AODV requires little bandwidth because the routing table and control data are very small.

(iii) It is very scalable.

In general, AODV uses four types of routing messages.

(i) *Route Request (RREQ).* This message is broadcasted by the source requesting the route and forwarded by the intermediate nodes if the message has not been processed before.

(ii) *Route Reply (RREP).* A message is sent to identify that a route has been found to the destination. This message is sent by a node; if it receives the RREQ message, it is the destination node or in the path of the destination node, and the message has a sequence number smaller than or equal to the one in the RREQ message.

(iii) *Route Error (RERR).* This message is sent by one of the nodes in the path used, source node, or destination node. The message is sent when the link breaks to notify the source to initiate the route discovery process again by broadcasting an RREQ message.

(iv) *Route Reply Acknowledgment (RREP-ACK).* This is used by the sender to ensure the availability of a link from the destination to the sender.

2.3. Comparison. The aforementioned reviews of secure routing protocols for WMN are summarized in Table 1, which highlights the core differences and limitations. These protocols vary in many respects, such as the mechanism architecture, tackled attacks, the technique used to detect the attacks, and efficiency. Four parameters are considered as limitations in the comparison below, which are complexity, requirement of additional resources, overhead, and efficiency of the protocol in protecting the network against attacks which might lead to DoS.

The comparison shows us that most secure routing protocols utilize cryptography [6, 9–12, 14, 16] to provide data security such as authentication, data confidentiality, and integrity over the network. Unfortunately, these protocols do not guarantee the protection of WMNs against the most important attacks, for example, selective forwarding, wormhole, and hello flooding [9, 11, 12], which jams data traffic and thus causes denial of service (DoS). Furthermore, some protocols [6, 8–10] assume that an authority already exists in the network to manage the distribution of certificates for data encryption.

Aside from cryptography and CA, two other types of solutions [5, 7, 8] have been proposed to handle the DoS problem: hardware-based and statistical-based solutions. In hardware-based solutions, GPS or an antenna is used to verify the location of a node and validate that it is legitimate neighbor [9]. In statistical-based solutions, the nodes keep track of their successful past communication with neighbors to select the best next hop [5, 7]. In general, solutions against attacks that target WMNs are still an open issue [2, 4, 17, 18].

3. Implementation and Results

The selection of the routing protocol to be used in the current research is critical since the study focuses on attacks on the routing protocol of WMNs.

3.1. Routing Protocols and Attacks. The selected routing protocol to be used in this study is AODV. AODV implementation is available for simulation tools, including OMNET++, which was selected to be used in simulation of these attacks because of its suitability [25].

In OMNET++, the INET framework facilitates the simulation and contains modules for wired and wireless communication, including the AODV routing protocol. INETMANET is an extension of the INET package that contains more routing protocols and standards related to mobility and wireless networks, including WMNs.

The second selected routing protocol is Position-Aware, Secure, and Efficient Mesh Routing (PASER). The reasons for selecting PASER for the current research are as follows.

(i) *Availability of Resources*. The PASER design and development team has put a great deal of effort into making the protocol available for researchers as well as for industry. This is reflected by the implementation of the protocol in C/C++ and integration for use in a Linux environment as a complete implementation where it can be ported and tested on real hardware or used in OMNET++ as a simulation package. For the simulation, it is available for OMNET++ for both Linux and Windows operating systems and integrated with the INET package. The only missing part of the resources is the availability of full documentation to describe in detail the PASER structure and how to use the protocol with OMNET++ packages.

(ii) *Usable Components*. The PASER design team used multiple components in their designs that are parts of other routing protocols or well-known packages, which makes the results of the study more accurate and trustworthy. In regard to routing methodology, PASER adapted the route discovery process from the AODV routing protocol. In addition, the route maintenance and detection process in PASER is adapted from the neighborhood discovery protocol (NHPS). Cryptographic primitives are a building block in PASER that were adapted from a well-known package in industry and academia, OpenSSL.

3.1.1. Hello Flooding Attacks. A hello flooding attack [26, 27] is a very destructive DoS attack. The malicious node tries to give itself a greater probability to be selected as a route by making itself more appealing. In wireless networks, this is usually accomplished by transmitting using a high power frequency to its neighbors, which causes the malicious node to cover a larger area and provide a shorter path to the destination [28]. After being selected as a node in the route, the malicious node then performs malicious activities on the received packets, such as altering packets or gain statistics or simply dropping the packets [29]. In the current research, the implementation of a hello flooding attack is performed as follows.

(i) *High Transmission Power*. The malicious node is configured to have higher transmission power than legitimate nodes. This is done by changing the .wlan* .radio.transmitterPower attribute in OMNET++ initialization file.

(ii) *Dropping the Packets*. The packets that go through the malicious node are simply dropped; this helps to gain more insightful information to study the effect of the attack. To do this correctly, the malicious node must drop only data packets, not routing and control packets; otherwise, the malicious node will not take part in the routing discovery process and will not be part of the route. Thus, the source code for the routing protocol in the malicious node must be altered by dropping the packets rather than forwarding them as shown in Algorithm 1.

3.1.2. Selective Forwarding Attack. A selective forwarding attack or grey hole attack is less destructive than a hello flooding attack because the malicious node has no advantage over legitimate nodes to be selected in the route. In a selective forwarding attack, the packets are forwarded inconsistently according to the attacker's goal [30], which can cause DoS in the network [31–33]. In the current research, the malicious node forwards the packets with a probability of 50%; otherwise, the packets will be dropped as shown in Algorithm 2.

Table 1: Comparison of the available solutions.

Reference	Mechanism	Tackled attacks	Security analysis	Limitations
WRSR [5]	Statistical based: neighbors' information and existing of alternative path	Wormhole	Simulation with strong adversary scenario	Inefficient protection due to limited number of attacks handled
WSRPHWM [6]	Cryptography based and past communication statistics	Spoofed route signaling Replay attack Black hole Wormhole Grey hole Routing disruption	Theoretical	(i) Additional resources are required which is a certification authority (ii) Overhead due to usage of public key cryptography
CSROR [7]	Past communication statistics	Wormhole, black hole, and grey hole	Not provided	Inefficient protection due to limited number of attacks handled
E-SRPM [8]	Link's length information and random walk route scheme	Wormhole	Simulation	Inefficient protection due to limited number of attacks handled
ARANA [9]	Cryptography based	Malicious packets manipulation	Simulation	(i) Additional resources are required which is a certification authority (ii) Overhead due to usage of public key cryptography (iii) Inefficient protection due to limited number of attacks handled
SAODV [10]	Cryptography based	Malicious packets manipulation of routing metric and nodes impersonation	Simulation	(i) Additional resources are required which is a certification authority (ii) Overhead due to usage of public key cryptography (iii) Inefficient protection due to limited number of attacks handled
I-SEAD [11]	Cryptography based	Malicious routing update	Simulation	Inefficient protection due to limited number of attacks handled
SAR [12]	Cryptography based	Route discovery process	Theoretical	(i) Additional resources are required which is a certification authority (ii) Overhead due to usage of public key cryptography (iii) Inefficient protection due to limited number of attacks handled
Leak detector [13]	Statistical based: neighbors' information and existence of alternative path	Selective forwarding and black hole	Simulation	(i) Inefficient protection due to limited number of attacks handled (ii) Complexity due to required integration in existing routing protocol
SeRWA [14]	Neighbor information and cryptography based	Wormhole	Simulation	(i) Additional resources are required to distribute keys (ii) Inefficient protection due to limited number of attacks handled
CRP [15]	Statistical based: neighbor information and public key cryptography	Black hole, grey hole, packet tampering, rushing attack, and collusion attack	Simulation	(i) Additional resources are required which is a certification authority (ii) Overhead due to usage of public key cryptography (iii) Inefficient protection due to limited number of attacks handled
PASER [16]	Cryptography based and GPS location	Wormhole and cryptographic protection (message and node authentication, message freshness, and message confidentiality)	Simulation	(i) Additional resources are required which is a certification authority and GPS hardware (ii) Overhead due to usage of public key cryptography

```
If (isHelloFlooding)
{
   if (dynamic_cast<UDPPacket *>(msg))
          {
             delete msg;
             return;
          }
}
```

Algorithm 1: Hello flooding attack implementation.

```
if (MIPs.equals(getAddress( ).getIPv4( )))
{
   if (uniform(0,1) < 0.5 & is Selective)
   {
      if (dynamic_cast<UDPPacket *>(msg))
          {
             delete msg;
             return;
          }
   }
}
```

Algorithm 2: Selective forwarding attack implementation.

3.1.3. Wormhole Attack. A wormhole is a more sophisticated attack that requires at least two malicious nodes to perform the attack by building wormhole tunnel [34]. This tunnel is usually built in wired networks by connecting a wire from the source to the destination; in the case of wireless communications the tunnel is built by having high-frequency overlapping coverage ranges for both the source and the destination [35, 36]. The source tries to be more attractive as a path selection for the packets by convincing its neighbors that it sees part of the network they cannot see which is a shorter path to the legitimate destination as shown in Figure 1. In the current research, the tunnel is built by high-frequency transmission power for both the tunnel source and destination.

3.2. Network Design and Parameters. This section describes the network parameters and configuration for the experiment. Table 2 shows the general configuration of the network, while Table 3 shows the specific network configuration related to the attack simulations. Tables 4 and 5 show the initial battery configuration and battery consumption parameters, respectively.

Figure 2 is the diagram that shows the initial layout and setup after configuring the above parameters.

The coverage of the radio signal in each node is a critical parameter in the research for the following reasons.

(i) It is used in routing protocol to find a path to the destination.

Table 2: General network configuration.

General configuration	
Simulation time	70,000 s
Number of nodes	50
Max area (x-axis)	1,000 M
Max area (y-axis)	1,000 M
Min area (x-axis)	0 M
Min area (y-axis)	0 M
Network layout for intermediate nodes	Random
Position for the source x-axis	1 M
Position for the source y-axis	1 M
Position for the destination x-axis	999 M
Position for the source y-axis	999 M

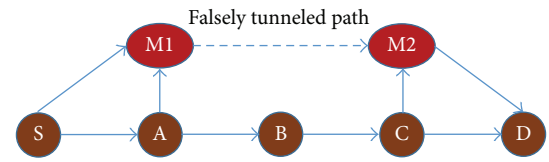

Figure 1: Wormhole attack description.

(ii) It is used by malicious nodes to attract other nodes to forward the traffic through them (in wormhole and hello flooding attacks).

Figure 3 shows the initial coverage of each node.

One of the goals of this research is to study the effect of mobility when malicious nodes are generating attacks in the network. For this reason, the mobility configuration plays a crucial part. The parameters of mobility for the two malicious nodes, which are numbered 1 and 2, are listed in Table 6.

3.3. Adversary Model. The adversary model and attacks scenarios as shown in Table 7 are performed on AODV and PASER protocols.

3.4. Simulation Scenarios with Malicious Nodes Performing a Hello Flooding Attack. In this section, the effect of a hello flooding attack on stationary and mobile networks is measured. The attack is performed by the transmission of high-frequency hello messages. Packet delivery ratio (PDR), throughput, and end-to-end delay are calculated and graphs are generated by Omnet++. After conducting attacks as described in Section 3.3, the collected results are shown in Table 8.

As Figure 4 shows, network PDR is strongly affected by hello flooding attack; the highest drop in PDR happened when attack scenario number 8 was conducted. This scenario caused PDR to decrease from 94.4% when the network does not contain any malicious node to reach 71.15% when eight mobile malicious nodes were conducting the attack. In summary, it can be said that the network PDR is strongly affected by hello flooding attack and the PDR decreases when the number of malicious nodes increases. Moreover, mobile

Table 3: Routing protocol parameters.

Network parameters	
Communication type	Wireless
MAC Protocol	IEEE 802.11g
Type of traffic	UDP
Routing protocol	AODV, PASER
Type of IP	IPv4
Source port	1234
Distention port	1234
Packet length	512 Bytes
IP forwarding	Enabled
IGMP type	IGMPv2
Packet time to live	32
Sending intervals	Random
Sleeping duration	1 second
Interface start time	10 seconds
Number of radio interface	1
Wireless NIC bitrate	54 Mbps
Wireless NIC frame capacity	10
Maximum queue size	14
Basic bitrate	6 Mbps
Sending retry limit	7
Radio maximum transmission power	20 mW
Maximum transmission power	6.0 mW
Default radio transmission power	2.0 mW
Radio sensitivity	−90 dBm
Broadcast delay	Random between 0 s and 0.005 s
Radio carrier frequency	2.4 GHz
Propagation model	Free space model

Table 4: Initial battery configuration.

Battery configuration	
Battery type	InetSimpleBattery
Battery nominal	25
Battery capacity	25
Battery voltage	10
Battery resolution	1 s
Delta value of battery	0.5
Battery publishing time	20 s
Battery consumption factors for radio and CPU	(i) Module is idle (ii) Module is asleep (iii) Module is sending packets (iv) Module is receiving packets (v) CPU is active (vi) CPU is standing by

Table 5: Battery consumption parameters.

Action	Cost
Radio, idle	1.3 mA
Radio, receive	9.0 mA
Radio, sleep	0.06 mA
Radio, send	9.0 mA

Table 6: Mobility configuration.

Node number	Mobility configuration	
Node number 1	Mobility Type	Circle mobility
	Radius	150 m
	Speed	100 mps
	Start Angle	120 degrees
	mobility.cy	250 m
	mobility.cx	250 m
Node number 2	Mobility Type	Constant speed mobility
	Speed	50 mps
Node number 3	Mobility Type	Circle mobility
	Radius	100 m
	Speed	80 mps
	Start Angle	120 degrees
	mobility.cy	250 m
	mobility.cx	250 m
Node number 4	Mobility Type	Constant speed mobility
	Speed	60 mps
Node number 5	Mobility Type	Constant speed mobility
	Speed	40 mps
Node number 6	Mobility Type	Constant speed mobility
	Speed	80 mps
Node number 7	Mobility Type	Constant speed mobility
	Speed	100 mps
Node number 8	Mobility Type	Circle mobility
	Radius	120 m
	Speed	90 mps
	Start Angle	90 degrees
	mobility.cy	100 m
	mobility.cx	100 m

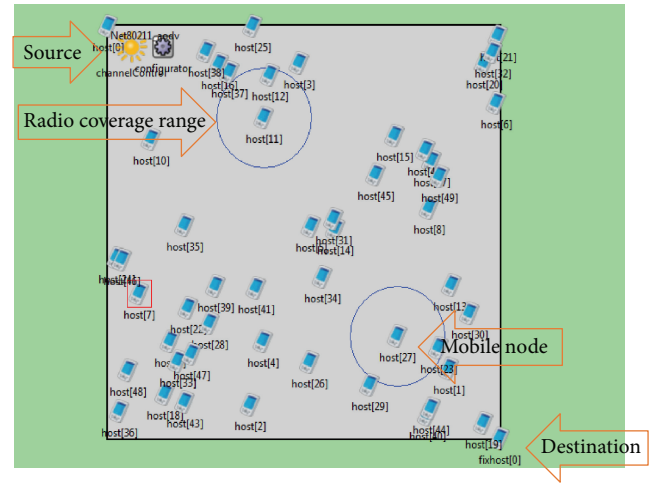

Figure 2: Initial layout of the network.

malicious nodes tend to cause more damage than stationary malicious nodes.

On the other hand, as shown in Figure 4, PASER showed very high PDR even when the network contained malicious nodes performing hello flooding attack. The highest PDR occurred when one stationary node performed the attack.

Table 7: Attacks' scenarios.

Attack	Scenario description	Scenario number
Selective forwarding and hello flooding	Network with one stationary malicious node	1
	Network with one mobile malicious node	2
	Network with two stationary malicious nodes	3
	Network with two mobile malicious nodes	4
	Network with four stationary malicious nodes	5
	Network with four mobile malicious nodes	6
	Network with eight stationary malicious nodes	7
	Network with eight mobile malicious nodes	8
Wormhole	Network where the source and the destination are stationary	9
	Network where the source is mobile and the destination is stationary	10
	Network where the source is stationary and the destination is mobile	11
	Network where the source and the destination are mobile	12

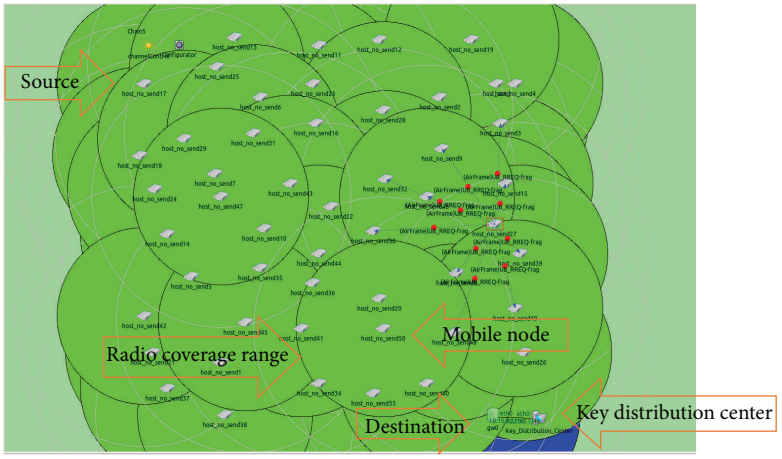

Figure 3: Radio coverage of nodes in the PASER based network.

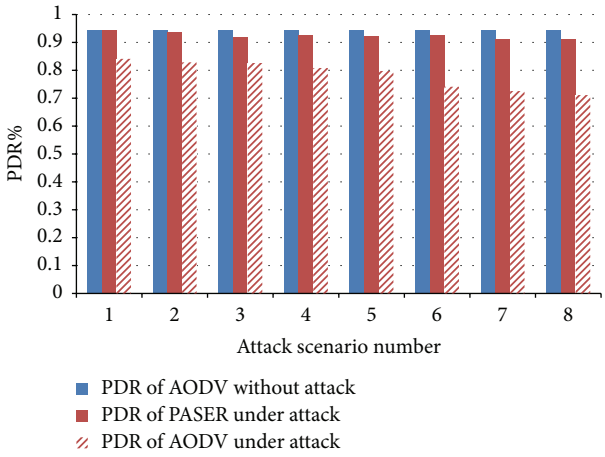

Figure 4: Impact of hello flooding attack on packet delivery ratio (PDR).

The lowest PDR was in scenario number 8; when eight malicious nodes were performing the attack, this caused only about 4.02% decrease in PDR. It can be said that PASER protocol when compared to AODV showed high PDR performance and immunity against hello flooding.

The effect of hello flooding attack on network throughput is not significant as shown in Figure 5. The largest drop was in the second case, where only one mobile node performed the attack. This decrease in throughput was only about 0.23%, which is not significant. The nature of the malicious nodes, whether they are mobile or stationary, does not affect the impact of the attack. In the first, second, fifth, and sixth attack scenarios, the mobile malicious nodes tend to cause more damage on network throughput. However, in the rest of attacks scenarios, the stationary malicious nodes caused greater decrease in network throughput. In general, network throughput is not significantly affected by hello flooding attack and mobility factor does not increase the damage caused by the attack.

The impact of implementing PASER as a security protocol appeared very clearly in network throughput, as shown in Figure 5. PASER achieved only about 56% of the throughput achieved by AODV when the two protocols were under hello flooding attack. This is because PASER uses authentication and cryptography to validate the packets, which slow down

Table 8: Results of hello flooding attacks on AODV and PASER.

Scenario number		Results with AODV	Results with PASER
1	Packet delivery ratio	84.10%	94.30%
	End-to-end delay	0.0038617 seconds	0.007586 seconds
	Throughput	9,309.219 bits/second	5,013.218 bits/second
2	Packet delivery ratio	82.86%	93.62%
	End-to-end delay	0.003969 seconds	0.007538 seconds
	Throughput	9,289.311 bits/second	5,010.701 bits/second
3	Packet delivery ratio	82.65%	92.08%
	End-to-end delay	0.004218 seconds	0.007812 seconds
	Throughput	9,308.361 bits/second	5,010.19 bits/second
4	Packet delivery ratio	80.85%	92.71%
	End-to-end delay	0.005643 seconds	0.007908 seconds
	Throughput	9,312.8620 bits/second	5,009.24 bits/second
5	Packet delivery ratio	79.80%	92.42%
	End-to-end delay	0.005712 seconds	0.007742 seconds
	Throughput	9,310.102 bits/second	5010.46 bits/second
6	Packet delivery ratio	74.13%	92.54%
	End-to-end delay	0.005811 seconds	0.007826 seconds
	Throughput	9,309.671 bits/second	5011.12 bits/second
7	Packet delivery ratio	72.54%	91.13%
	End-to-end delay	0.006105 seconds	0.007691 seconds
	Throughput	9,306.418 bits/second	5004.17 bits/second
8	Packet delivery ratio	71.15%	91.31%
	End-to-end delay	0.006412 seconds	0.007781 seconds
	Throughput	9,308.369 bits/second	4981.71 bits/second

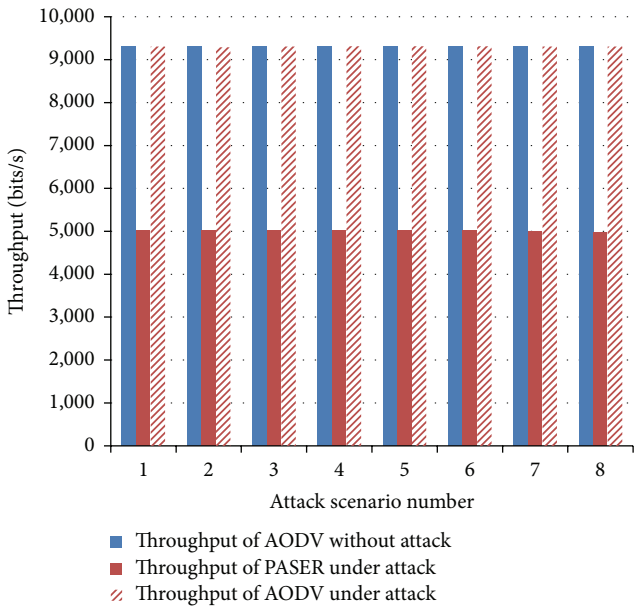

Figure 5: Impact of hello flooding attack on throughput.

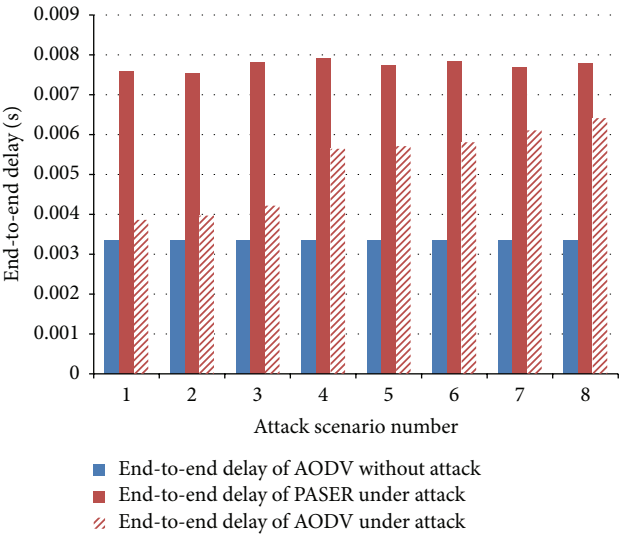

Figure 6: Impact of hello flooding attack on end-to-end delay.

the forwarding of data and routing packets. The mobility of malicious nodes did not affect the performance of PASER in protecting the network.

The impact of hello flooding attack on end-to-end delay is tangible and serious. Figure 6 shows that the effect of hello flooding attack increases when the number of malicious nodes increases, which is clear in all eight attack scenarios. Moreover, the impact of hello flooding attack on network end-to-end delay was more destructive when malicious mobile nodes performed the attack. The most significant increase in end-to-end delay took place when eight mobile malicious nodes performed the attack. In this case, the end-to-end delay increased by 91.52%, which is very high. The lowest increase in end-to-end delay took place when only one

Table 9: Results of selective forwarding attack on AODV and PASER.

Scenario number		Results with AODV	Results with PASER
1	Packet delivery ratio	87.10%	95.10%
	End-to-end delay	0.003495 seconds	0.007532 seconds
	Throughput	9,310.12 bits/second	5,012.81 bits/second
2	Packet delivery ratio	86.22%	94.64%
	End-to-end delay	0.003550 seconds	0.007698 seconds
	Throughput	9,302.11 bits/second	5,009.31 bits/second
3	Packet delivery ratio	86.13%	93.21%
	End-to-end delay	0.003701 seconds	0.007721 seconds
	Throughput	9,308.88 bits/second	5,011.45 bits/second
4	Packet delivery ratio	85.13%	91.13%
	End-to-end delay	0.00446 seconds	0.008101 seconds
	Throughput	9,301.356 bits/second	5,012.04 bits/second
5	Packet delivery ratio	83.21%	92.61%
	End-to-end delay	0.00529 seconds	0.007915 seconds
	Throughput	9,294.21 bits/second	5008.12 bits/second
6	Packet delivery ratio	82.40%	91.84%
	End-to-end delay	0.005321 seconds	0.008101 seconds
	Throughput	9,300.81 bits/second	5,010.52 bits/second
7	Packet delivery ratio	81.74%	91.72%
	End-to-end delay	0.005983 seconds	0.008106 seconds
	Throughput	9,276.47 bits/second	5,001.12 bits/second
8	Packet delivery ratio	81.13%	90.82%
	End-to-end delay	0.006018 seconds	0.008120 seconds
	Throughput	9285.18 bits/second	4,981.87 bits/second

malicious stationary node performed the attack; the increase in this situation was about 15.3%.

As Figure 6 shows, PASER caused higher end-to-end delay on the network compared to AODV when the network was under hello flooding attack. This was not an effect of the attack since the increase in the number of malicious nodes was not reflected in end-to-end delay; rather, it was associated with how PASER selects the optimal path and the time taken to validate the position of the nodes and to validate routing packets.

Since, AODV does not contain any protection mechanism and at packet loss performs route discovery. This is good in terms of throughput and end-to-end delay, but not in case of PDR. On the other hand, PASER is security protocol which is based on cryptography, mainly public/key cryptography that makes throughput and end-to-end delay of each node low, as each node has to verify the signature of the packet and then resign and forward it, but provides better PDR and thus improves the efficiency of the MWMN as shown in Figures 4, 5, and 6.

3.5. Simulation Scenarios with Malicious Nodes Performing a Selective Forwarding Attack. In this section, the effect of a selective forwarding attack on stationary and mobile networks is measured. The attack is performed by malicious nodes randomly dropping packets. The scenarios described in Section 3.3 were simulated and the collected results are shown in Table 9. The collected results then were compared to the results of AODV under the same attack.

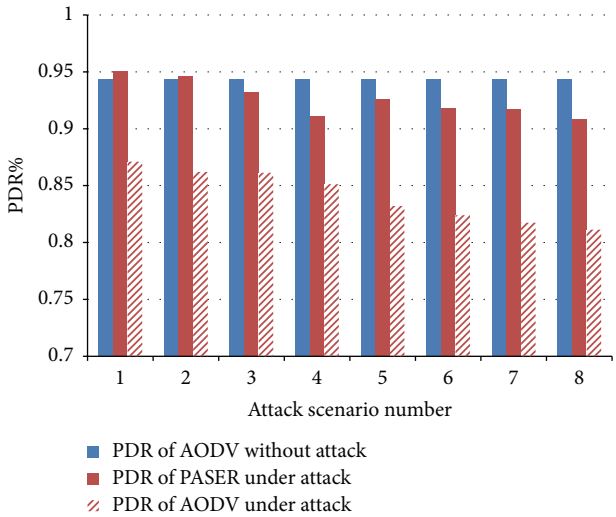

Figure 7: Impact of selective forwarding attack on packet delivery ratio (PDR).

As Figure 7 shows, even though selective forwarding attack is less harmful than hello flooding attack, it still causes significant decrease in network PDR. The worst case took place when scenario number 8 was conducted; this caused 16.36% drop in network PDR. By comparing all eight scenarios, it became clear that mobile malicious nodes introduced more damage.

Table 10: Results of wormhole attack on AODV and PASER.

Test scenario		Results with AODV	Results with PASER
9	Packet delivery ratio	84.81%	96.23%
	End-to-end delay	0.003861 seconds	0.007761 seconds
	Throughput	9,303.54 bits/second	5,012.31 bits/second
10	Packet delivery ratio	84.10%	95.71%
	End-to-end delay	0.004015 seconds	0.007532 seconds
	Throughput	9,289.51 bits/second	5,011.72 bits/second
11	Packet delivery ratio	85.90%	95.03%
	End-to-end delay	0.003928 seconds	0.007891 seconds
	Throughput	9,313.64 bits/second	5,010.68 bits/second
12	Packet delivery ratio	85.13%	94.21%
	End-to-end delay	0.003987 seconds	0.007961 seconds
	Throughput	9,301.11 bits/second	5,012.36 bits/second

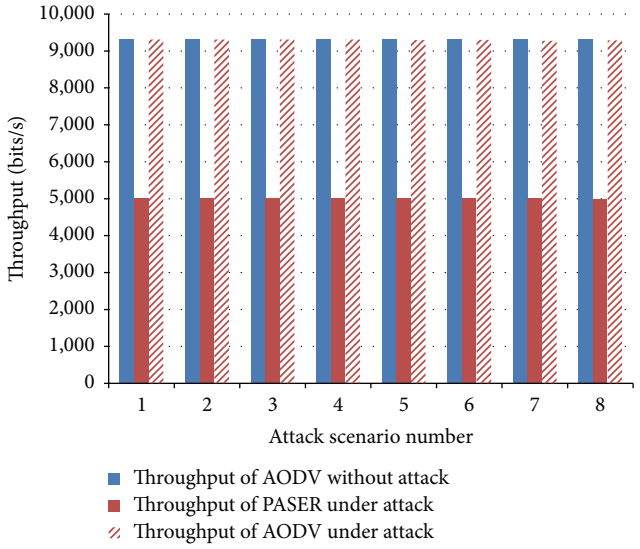

Figure 8: Impact of selective forwarding attack on throughput.

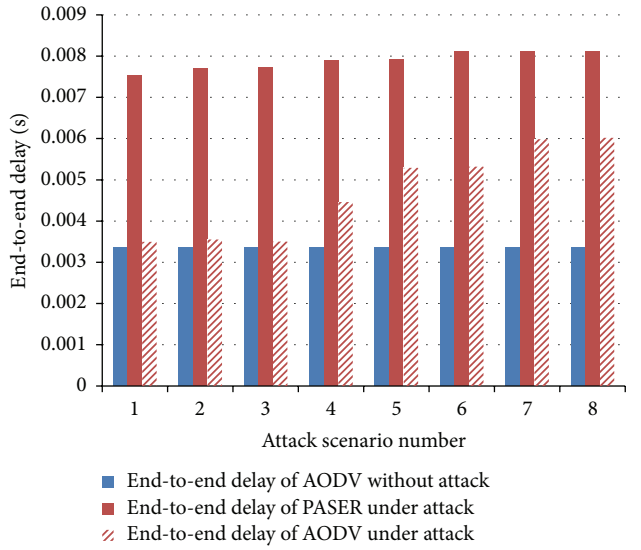

Figure 9: Impact of selective forwarding attack on end-to-end delay.

When the network was under selective forwarding attack, PASER still showed high PDR compared to AODV as shown in Figure 7. The lowest PDR for both routing protocols occurred when eight mobile malicious nodes performed the attack. In selective forwarding attack, the impact of the mobility factor was stronger, especially when eight malicious nodes performed the attack. This is clear by comparing each stationary attack scenario with mobile attack scenario for the same number of malicious nodes.

Figure 8 shows that the impact of selective forwarding attack and mobility is not significant in network throughput. The largest drop in throughput was from 9310.891 bits/second to 9276.47 bits/second when eight stationary nodes were involved in the attack. This drop was only about 0.37%.

The throughput of PASER network under selective forwarding attack was about 53.7% of AODV throughput under the same attack, as shown in Figure 8, which was approximately the same impact of hello flooding attack. Figure 8 also shows that the impact of the mobility of malicious nodes was minor.

In case of AODV as shown in Figure 9, the impact of mobile malicious nodes performing selective forwarding attack on end-to-end delay is more significant than the impact caused by stationary malicious nodes. The eighth attack scenario where the malicious nodes are mobile caused largest increase in end-to-end delay with about 79.75% increase.

End-to-end delay of PASER network under selective forwarding attack is high compared with AODV. As shown in Figure 9, end-to-end delay of PASER network was more than the double of end-to-end delay caused by AODV network under the same attack. In general, even though the difference was high, the mobile malicious nodes caused higher end-to-end delay in both AODV and PASER based networks.

3.6. Simulation Scenarios with Malicious Nodes Performing a Wormhole Attack. In this section, the impact of wormhole attack on stationary and mobile networks is measured; after conducting the attacks as described in Section 3.3, the collected results are shown in Table 10.

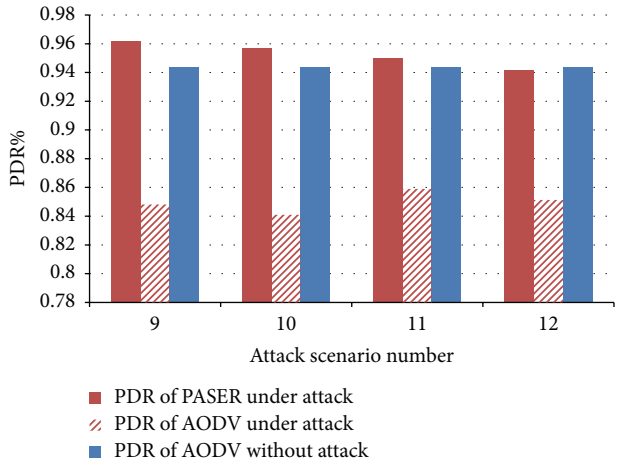

Figure 10: Impact of wormhole attack on packet delivery ratio (PDR).

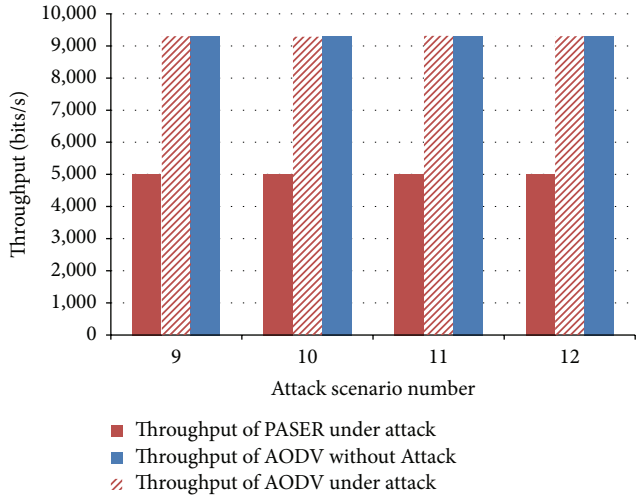

Figure 11: Impact of wormhole attack on throughput.

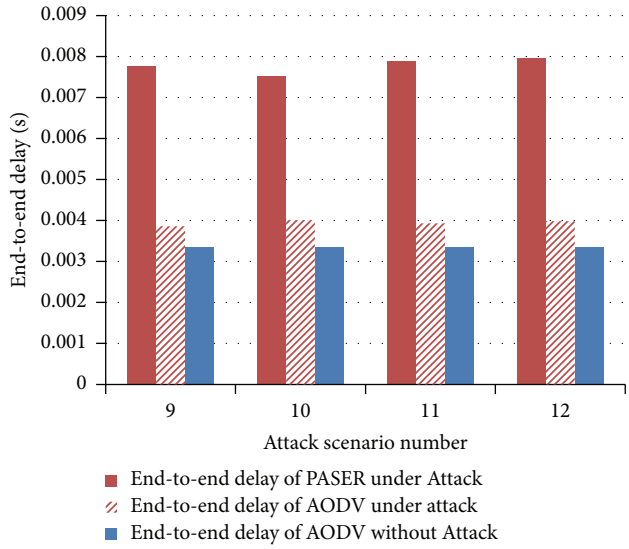

Figure 12: Impact of wormhole attack on end-to-end delay.

Figure 10 shows that the impact of wormhole attack on PDR was more significant when there is mobility in the network. The highest decrease in the PDR is about 11.22% which took place when the source of the wormhole is mobile and the destination is stationary. Moreover, Figure 10 also shows that when the source and the destination of the wormhole were stationary, the impact of the wormhole attack on the PDR was of slightly less than 10.15% drop. It can be concluded that the mobility of malicious nodes makes the impact of wormhole attack more destructive.

Moreover, as shown in Figure 10, PASER showed immunity to wormhole attack because of the usage of cryptography to authenticate packets and usage of GPS to validate nodes locations. The PDR achieved by PASER was very high compared with the PDR achieved by AODV. The highest difference in PDR between AODV and PASER took place when the source of the wormhole tunnel was stationary and the destination was mobile. In this case, PASER achieved 12.8% higher PDR. In regard to mobility, PASER was not affected by the mobility of the malicious nodes.

As Figure 11 shows, in case of AODV the impact of a wormhole attack on throughput was not significant. In the worst case, when the source of the wormhole was mobile and the destination of the wormhole was stationary, the decrease in throughput in this case was about 0.23%. Moreover, the results show that the mobility of malicious nodes did not increase the damage caused by the attack. This was found by comparing the first setup, where both ends of the tunnel were stationary with the fourth setup and where both ends of the tunnel were mobile.

In case of PASER, the throughput of the network when a wormhole attack occurs in the network was approximately the same as that with the selective forwarding and hello flooding attacks, as shown in Figure 11. AODV still achieved more than double the throughput achieved by PASER under the same type of attack. The highest difference in throughput took place in the third scenario, when the source of the wormhole was mobile and the destination was stationary. In this case, the throughput achieved by AODV was 9,313.64 bits/second, while PASER achieved 5,010.68 bits/second, a decrease of about 85.87% in network throughput.

The results presented in Figure 12 shows that the damage caused by wormhole attack is very significant with respect to end-to-end delay. The highest increase in end-to-end delay took place when the source of the tunnel was mobile and the destination was stationary; the increase was about 19.92%. Moreover, the mobility of malicious nodes made the impact of wormhole attack more significant. This was concluded by comparing the increase in end-to-end delay when the wormhole tunnel ends were both stationary with the scenario when the wormhole tunnel ends were mobile. In the first case, the increase in end-to-end delay was about 15%, while it was about 19% in the second case.

In case of PASER, end-to-end delay in PASER network as shown in Figure 12 was affected more by wormhole attack than by selective forwarding and hello flooding attacks. The

Table 11: PDR of AODV and PASER in large networks.

Number of nodes	PDR (%) with AODV	PDR (%) with PASER
50	94.40	94.83
75	93.25	94.41
100	90.21	93.16
125	88.56	92.52
150	76.15	91.08
175	91.3	91.91
200	71.86	90.78
225	80.48	92.36
250	88.14	91.73
275	91.28	92.75
300	75.43	86.31

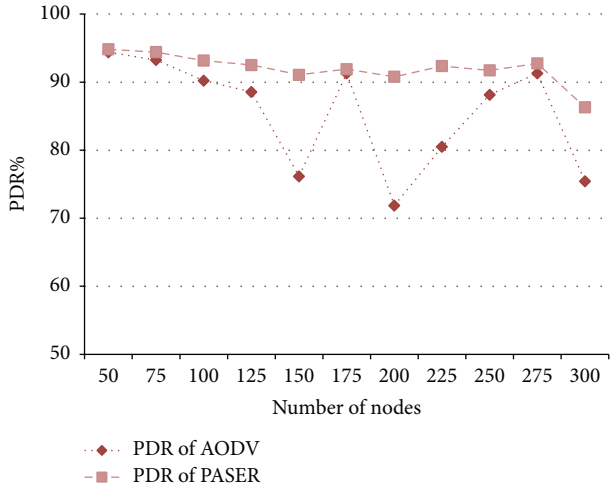

Figure 13: PDR of PASER and AODV in large networks.

Table 12: Throughput of AODV and PASER in large networks.

Number of nodes	Throughput (bits/seconds) with AODV	Throughput (bits/seconds) with PASER
50	9310.891	5200.471
75	9301.413	5112.671
100	9289.21	4981.325
125	9309.77	4627.268
150	9084.18	4489.772
175	9101.46	4413.271
200	9101.83	4106.471
225	9281.93	3819.446
250	9011.71	3528.731
275	8980.76	3187.267
300	9012.14	2967.164

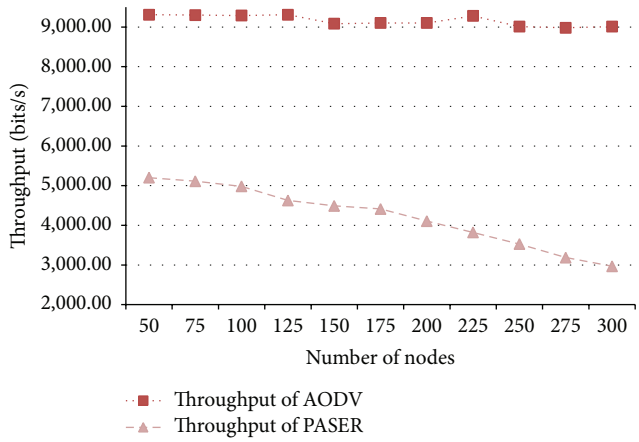

Figure 14: Throughput of PASER and AODV in large networks.

highest end-to-end delay took place when both ends of the wormhole tunnel were mobile, which is double the end-to-end delay of AODV in the same circumstances.

3.7. Performance and Scalability. After studying the impact and immunity of AODV and PASER against attacks and the impact of these attacks on performance, in this section, PASER and AODV routing protocol are tested in larger network in the same circumstances as elaborated with the number of nodes being increased from 50 to 300 nodes with increment of 25 nodes in each experiment. The attributes to be measured are PDR, end-to-end delay, and network throughput. Moreover, this section will compare the performance and scalability of both AODV and PASER.

3.7.1. Impact on Network PDR. After measuring PDR of AODV and PASER based networks while varying the nodes from 50 to 300, the collected results are listed in Table 11.

As Figure 13 shows PDR of AODV protocol varies from 94.4% to 71.86%. In the case of AODV, it can be seen that when the number of nodes increases, PDR decreases due to the increase of collision between packets when travelling from source to destination. As shown in Figure 13, PASER showed very high PDR compared to AODV in all experiments. Moreover, PASER shows very good scalability and performance of PDR when compared with AODV. The lowest reading for PASER was 86.31% when the network contains 300 nodes; the rest of reading shows that the highest network PDR drop was not more than 4.46%. On the other hand AODV PDR dropped from 94.4% to reach 71.86% when the network contains 200 nodes.

3.7.2. Impact on Network Throughput. Network throughput was measured with different network sizes for AODV and PASER as shown in Table 12. The measured values of network throughput for routing protocols are listed in Table 12.

When considering network throughput, PASER showed continuous decrease when the number of nodes increases as shown in Figure 14. The lowest throughput of PASER protocol was 2967.164 bits/second which took place when the number of nodes is 300. This is due to the increase of routing packets when the number of nodes increases, which leads to increase in signing and verification process of routing packets.

Table 13: End-to-end delay of AODV and PASER in large networks.

Number of nodes	End-to-end delay (seconds) with AODV	End-to-end delay (seconds) with PASER
50	0.003348	0.0074
75	0.003421	0.007501
100	0.003762	0.007513
125	0.003901	0.007978
150	0.003978	0.008102
175	0.003851	0.00821
200	0.004021	0.00861
225	0.004089	0.00887
250	0.004147	0.00916
275	0.004162	0.00971
300	0.004189	0.01073

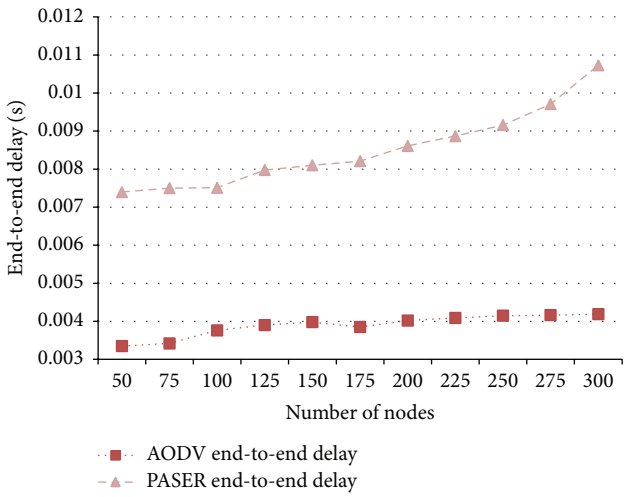

Figure 15: End-to-end delay of PASER and AODV in large networks.

3.7.3. Impact on Network End-to-End Delay. The measured values of network end-to-end delay for AODV and PASER routing protocols are listed in Table 13.

According to Figure 15, network end-to-end delay increased by 25.11% in the worst case. The lowest end-to-end delay took place when the network size was only 50 nodes with value of 0.003348 seconds, while the longest end-to-end delay was 0.004189 seconds when the number of nodes is 300. Such increase in end-to-end delay is affected by the route discovery process and number of nodes in the path from the source to destination.

The collected results of network end-to-end delay showed that PASER causes increase in end-to-end delay when the number of nodes increases. As shown in Figure 15, the increase reached about 45% in the worst case. Comparing this by AODV results shows that AODV is more scalable and can deliver better end-to-end delay performance.

4. Discussion and Recommendations

One of the goals of this research is to study the effect of hello flooding, selective forwarding, and wormhole attacks on network performance, particularly the effect on PDR, network throughput, and end-to-end delay. Table 14 shows the effect of each attack on each network parameter for both routing protocols under study. The PDR and end-to-end delay were the most affected network parameters by the attacks, while throughput was less affected. Moreover, Table 14 shows the results of using PASER to protect the network against these three types of attacks. PASER was successful in reducing the impact of all three attacks on network PDR. In regard to end-to-end delay and network throughput, PASER was able to protect the network against the attacks, but unfortunately it introduced more end-to-end delay and reduced network throughput as shown in Sections 3.4, 3.5, 3.6, and 3.7. This is due to the heavy usage of cryptography by PASER in authenticating nodes and routing packets, which led to substantial increase in end-to-end delay and decrease in network throughput.

One of the main contributions of this research is to study the impact of mobility of malicious nodes in network performance. Table 15 shows the association between the mobility of malicious nodes and level of damage caused by attack. Here, Yes means that the mobile malicious nodes caused more damage than stationary nodes, while No indicates that mobile nodes did not cause more damage than stationary nodes. As Table 15 shows, mobile nodes tended to increase the effect of attack on network PDR for AODV protocol more than in PASER except for selective forwarding attack. In regard to end-to-end delay, the effect of the attacks on both protocols increased when the malicious nodes were mobile.

The performance decrease and weak scalability of PASER protocols reveal the need for a protection mechanism to detect and isolate malicious nodes without continuous authentication. Such mechanism can be integrated into the route discovery process and used in the detection and repair of broken routes. A statistical-based methodology that uses routing history to select the safest route is an option to be considered, but it requires determining how to select the route for the first time and how the exchanged and saved routing data will affect network and nodes performance. A hybrid approach which uses cryptography and communication statistics is also worth considering. In such approach, routing protocol can use cryptography to authenticate packets and nodes to guarantee the connectivity and existence of an alternative path while gathering statistics to provide the faster path when required.

5. Conclusion and Future Work

Denial-of-service (DoS) attacks are fatal to many types of network, including wireless mesh networks, specifically when the network is utilized in a highly sensitive scenario like eHealthcare. This paper focused on studying three types of attacks that can cause DoS in static and mobile WMNs: hello flooding, selective forwarding, and wormhole attacks. The first step was to study the available solutions for DoS attacks on WMNs. The literature review indicates that there is no routing protocol that provides a comprehensive solution for the DoS problem in WMNs. In general, the proposed solutions tend to deal with a specific attack or a group of

Table 14: Impact of all attacks on network parameters.

Routing protocol	Attack	Network parameter		
		PDR	Throughput	End-to-end delay
AODV	Hello flooding	−32.68%	−0.23%	+91.52%
	Selective forwarding	−16.36%	−0.37%	+79.75%
	Wormhole	−11.22%	−0.23%	+19.92%
PASER	Hello flooding	−4.02%	−0.94%	+6.86%
	Selective forwarding	−4.10%	−0.93%	+9.73%
	Wormhole	−0.67%	−0.35%	+7.58%

Table 15: Impact of mobility of malicious nodes on AODV and PASER.

Routing protocol	Attack	Network parameter		
		PDR	Throughput	End-to-end delay
AODV	Hello flooding	Yes	No	Yes
	Selective forwarding	Yes	No	Yes
	Wormhole	Yes	No	Yes
PASER	Hello flooding	No	No	Yes
	Selective forwarding	Yes	No	Yes
	Wormhole	No	No	Yes

attacks without being able to secure the routing layer completely. Most of the proposed solutions utilize cryptography to authenticate routing packets and neighboring nodes, which assumes that nodes can register with an authority to obtain certificates and validate themselves. Moreover, it assumes that these nodes will not perform malicious activities. The second proposed methodology is to use past communication statistics to identify malicious nodes that are trying to disrupt the network. Hardware-based solutions are also suggested to solve wormhole attacks.

To implement the attacks and measure their effect, it was necessary first to select the routing protocol to be used in the network layer of a WMN. AODV, a very common routing protocol, was selected to be analyzed, and its immunity to the effect of these attacks on the packet delivery ratio, throughput, and end-to-end delay of the network was measured. To perform this task, OMNET++, a simulation tool, was selected to implement the three types of attacks and launch them against a mobile WMN. In general, the results showed that the significantly affected network performance parameters were the PDR and throughput.

After determining the impact of the attacks on AODV, the next step was to decide which security protocol to use as defense protocol against the attacks. One of the mature proposed solutions selected was Position-Aware, Secure, and Efficient Mesh Routing (PASER). PASER routing protocol depends heavily on public key cryptography to secure routing by authenticating routing packets and nodes. Moreover, PASER uses a GPS module to validate nodes' locations to detect wormhole tunnels and prevent attacks. The results show that PASER is very effective in protecting the network against attacks, but, unfortunately, it imposes a performance cost on the PDR and end-to-end delay because of the heavy usage of cryptography. Moreover, PASER assumes the existence of a key distribution center (KDC) to issue keys for the nodes, which might not always be possible, and prevents the dynamic enrollment of nodes in the WMN.

During the process of writing this paper, it became clear that there is room for future improvement and enhancement, as the literature lacks solid implementation and simulation modules for all types of attacks to be used in testing and evaluating new proposed solutions. Providing such a framework will help researchers to provide practical solutions. Reviewing the proposed solutions reveals that designing a smart detection mechanism that does not depend on cryptography to detect and isolate malicious nodes is very helpful and will help in advancing WMN security research. In the future, these types of mechanisms and protocols for detecting malicious nodes can be investigated, and their effectiveness in protecting the network can be studied.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This project was funded by the National Plan of Science, Technology and Innovation (MAARIFAH), King Abdulaziz City for Science and Technology, Saudi Arabia (Award no. 12-INF2817-02).

References

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer Networks*, vol. 47, no. 4, pp. 445–487, 2005.

[2] P. H. Pathak and R. Dutta, "A survey of network design problems and joint design approaches in wireless mesh networks," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 3, pp. 396–428, 2011.

[3] S. D. Odabasi and A. H. Zaim, "A survey on wireless mesh networks, routing metrics and protocols," *International Journal of Electronics, Mechanical and Mechatronics Engineering*, vol. 2, no. 1, pp. 92–104, 2010.

[4] C.-W. Lee, "Security in wireless mesh networks," in *Wireless Network Security*, pp. 229–246, Springer, Berlin, Germany, 2013.

[5] R. Matam and S. Tripathy, "WRSR: wormhole-resistant secure routing for wireless mesh networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, article 180, 2013.

[6] Z. You and Y. Wang, "An efficient and secure routing protocol for a hybrid wireless mesh network," *Journal of Computational Information Systems*, vol. 8, no. 21, pp. 8693–8705, 2012.

[7] S. Khan and J. Loo, "Cross layer secure and resource-aware on-demand routing protocol for hybrid wireless mesh networks," *Wireless Personal Communications*, vol. 62, no. 1, pp. 201–214, 2012.

[8] S. Khan, N. A. Alrajeh, and K.-K. Loo, "Secure route selection in wireless mesh networks," *Computer Networks*, vol. 56, no. 2, pp. 491–503, 2012.

[9] D. Benetti, M. Merro, and L. Viganò, "Model checking ad hoc network routing protocols: ARAN vs. endair A," in *Proceedings of the 8th IEEE International Conference on Software Engineering and Formal Methods (SEFM '10)*, pp. 191–202, September 2010.

[10] S. Lu, L. Li, K.-Y. Lam, and L. Jia, "SAODV: a MANET routing protocol that can withstand black hole attack," in *Proceedings of the International Conference on Computational Intelligence and Security (CIS '09)*, pp. 421–425, Beijing, China, December 2009.

[11] C. H. Lin, W. S. Lai, Y. L. Huang, and M. Chou, "I-SEAD: a secure routing protocol for mobile Ad Hoc networks," *Multimedia and Ubiquitous Engineering*, vol. 1, no. 1, pp. 102–107, 2008.

[12] M. O. Pervaiz, M. Cardei, and J. Wu, "Routing security in Ad Hoc wireless networks," *Network Security*, pp. 117–142, 2010.

[13] K. Graffi, P. S. Mogre, M. Hollick, and R. Steinmetz, "Detection of colluding misbehaving nodes in mobile ad hoc and wireless mesh networks," in *Proceedings of the 50th Annual IEEE Global Telecommunications Conference (GLOBECOM '07)*, pp. 5097–5101, Washington, DC, USA, November 2007.

[14] S. Madria and J. Yin, "SeRWA: a secure routing protocol against wormhole attacks in sensor networks," *Ad Hoc Networks*, vol. 7, no. 6, pp. 1051–1063, 2009.

[15] H.-M. Sun, C.-H. Chen, C.-W. Yeh, and Y.-H. Chen, "A collaborative routing protocol against routing disruptions in MANETs," *Personal and Ubiquitous Computing*, vol. 17, no. 5, pp. 865–874, 2013.

[16] M. Sbeiti, A. Wolff, and C. Wietfeld, "PASER: Position aware secure and efficient route discovery protocol forwireless mesh networks," in *Proceedings of the 5th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE '11)*, pp. 63–70, Saint Laurent du Var, France, August 2011.

[17] A. Sgora, D. D. Vergados, and P. Chatzimisios, "A survey on security and privacy issues in wireless mesh networks," *Security and Communication Networks*, 2013.

[18] J. Sen, "Security and privacy issues in wireless mesh networks: a survey," in *Wireless Networks and Security*, Signals and Communication Technology, pp. 189–272, Springer, Berlin, Germany, 2013.

[19] S. Alanazi, J. Al-Muhtadi, A. Derhab et al., "On resilience of Wireless Mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications," in *Proceedings of the 17th International Conference on E-Health Networking, Application & Services (HealthCom '15)*, pp. 205–210, IEEE, Boston, Mass, USA, October 2015.

[20] S. M. S. Bari, F. Anwar, and M. H. Masud, "Performance study of hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11s WLAN mesh networks," in *Proceedings of the International Conference on Computer and Communication Engineering (ICCCE '12)*, pp. 712–716, July 2012.

[21] M. Shivlal and S. Kumar, "Performance analysis of secure wireless mesh networks," *Research Journal of Recent Sciences*, vol. 1, no. 3, pp. 80–85, 2012.

[22] T.-M. Hoang, V.-L. Dinh, and K.-Q. Nguyen, "A study on routing performance of 802.11 based wireless mesh networks under serious attacks," in *Proceedings of the IEEE International Conference on Computing, Management and Telecommunications (ComManTel '13)*, pp. 295–297, Ho Chi Minh City, Vietnam, January 2013.

[23] S. Bhumireddy, S. Tripathy, and R. Matam, "Secure peer-link establishment in wireless mesh networks," *Advances in Intelligent Systems and Computing*, vol. 176, no. 1, pp. 189–198, 2012.

[24] C. Perkins, E. Belding-Royer, and D. Samir, *Ad Hoc on Demand Distance Vector (AODV) Routing (RFC 3561)*, IETF MANET Working Group, 2003.

[25] P. Owczarek and P. Zwierzykowski, "Review of simulators for wireless mesh networks," *Journal of Telecommunications & Information Technology*, vol. 2014, no. 3, pp. 82–89, 2014.

[26] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 85–91, 2007.

[27] N. S. Chouhan and S. Yadav, "Flooding attacks prevention inMANET," *International Journal of Computer Technology and ElectronicsEngineering (IJCTEE)*, vol. 1, no. 3, 2011.

[28] M. O. Khozium, "Hello flood countermeasure for wireless sensor networks," *International Journal of Computer Science and Information Security*, vol. 2, no. 3, pp. 57–65, 2008.

[29] U. Khartad and R. K. Krishna, "Route request flooding attack using trust based security scheme in Manet," *International Journal of Smart Sensors and Ad Hoc Networks*, vol. 1, no. 4, pp. 27–33, 2012.

[30] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in WMNS," *IEEE Transactions on Wireless Communications*, vol. 9, no. 5, pp. 1661–1675, 2010.

[31] P. Zhou, Z. Xiang, and Y. Chen, "Detection method of gray-hole node in wireless mesh networks," in *Proceedings of the 5th International Conference on Computational and Information Sciences (ICCIS '13)*, pp. 1570–1573, IEEE, Shiyang, China, June 2013.

[32] L. Lazos and M. Krunz, "Selective jamming/dropping insider attacks in wireless mesh networks," *IEEE Network*, vol. 25, no. 1, pp. 30–34, 2011.

[33] S. Khanam, H. Y. Saleem, and A. K. Pathan, "An efficient detection model of selective forwarding attacks in wireless mesh networks," in *Internet and Distributed Computing Systems*, pp. 1–14, Springer, Berlin, Germany, 2012.

[34] A. A. Bhosle, T. P. Thosar, and S. Mehatre, "Black-hole and wormhole attack in routing protocol AODV in MANET," *International Journal of Computer Science, Engineering and Applications (IJCSEA)*, vol. 2, no. 1, pp. 45–54, 2012.

[35] R. Maulik and N. Chaki, "A study on wormhole attacks in MANET," *International Journal of Computer Information Systems and Industrial Management Applications*, vol. 3, no. 2, pp. 271–279, 2011.

[36] J. D. Parmar, A. D. Patel, R. H. Jhaveri, and B. I. Shah, "MANET routing protocols and wormhole attack against AODV," *International Journal of Computer Science and Network Security*, vol. 10, no. 4, pp. 12–18, 2010.