Preamble time-division multiple access fixed slot assignment protocol for secure mobile ad hoc networks

Khalid Hussain Mohammadani1, Kamran Ali Memon2, Imran Memon3, Nazish Nawaz Hussaini4 and Hadiqua Fazal3

Abstract
Mobile ad hoc networks are the "spontaneous networks" which create a temporary network in any place and any time without using any extra fixed radio device of a full infrastructure network. Each device in this network works as a router to develop end-to-end communication connections and move independently in any direction. Mostly, mobile ad hoc networks use the IEEE 802.11b protocol with carrier-sense multiple access with collision avoidance medium access control layer protocol for sharing a common medium among the nodes simultaneously. Due to this distributed medium, the routing and medium access control layer of the mobile ad hoc network are prone to attacks. Among several attackers, blackhole attacker is the dangerous one which causes the loss of all data packets of devices in the network. Efficient medium access control protocol designs in this respect play a key role in determining channel utilization, network delay, and, more importantly, network security. In the proposed work, preamble information is used with time-division multiple access medium access control. The preamble time-division multiple access uses time synchronization for each time slot and does not assign much time to the blackhole attacker due to a fixed time slot. As a result, blackhole is not stable in all communications and such an attack is effectively defended. Simulation results show that, in the presence of the blackhole attacker, carrier-sense multiple access with collision avoidance has a high packet loss ratio and low network throughput as compared to the proposed preamble time-division multiple access.

Keywords
Mobile ad hoc network, blackhole attack, carrier-sense multiple access, time-division multiple access

Date received: 7 January 2020; accepted: 27 March 2020

Handling Editor: Pascal Lorenz

Introduction
Since decades, the demand of mobile/wireless subscribers has been increasing rapidly due to the extensive use of bandwidth-hungry applications such as video on demand (VoD), on-line gaming, and BitTorrent.1 Infrastructure-full and infrastructure-less communications are two main types of wireless communication to support high data rates for a wireless medium in this case. Infrastructure-full communication2 is known as single-hop communication (e.g. GSM (Global System for Mobile Communications), CDMA (code-division...
multiple access), LTE (Long-Term Evolution), etc.) or as the terrestrial fixed wireless network. Infrastructure-full network is a fixed network where the end-to-end route is established by some fixed base stations or access points, as shown in Figure 1. The base stations and access points are connected with the backbone network via microwave or optical fiber. Due to some excellent features (such as the mobility of end users), the infrastructure-full network had replaced the wired network.3 Furthermore, end users can communicate during movement due to the handover/handoff process, but the movement is limited to be within the network coverage area of base stations. In addition, the coverage area can also be increased using the concept of the terrestrial multi-hop network at last miles.4–6 The infrastructure-full network is a more secure wireless network due to its central management technique. Therefore, attackers do not easily attack it. If any attacker attacks on this network, the central management technique handles attacks and safeguards this network.

The infrastructure-less network, on the other hand, is established without any base station or access point of wireless network where end users do not require any central fixed device for establishing the network. Mobile ad hoc network (MANET) is one of the fastest developed research areas in the wireless network.7,8 MANET is a self-configuring and dynamic network with a large number of portable devices.9 MANET’s nodes create a temporary and dynamic network of portable devices such as laptops, mobiles, and printers with wireless links (Figure 2). There is no pre-defined wireless route established among the MANET’s nodes. Therefore, each device has its routing capability10 and nodes create trust levels on each other. These nodes can easily move up in their set wireless range.11

Due to its nature of the infrastructure-less and open network structure, there are so many issues and limitations in MANET as well,12–15 such as challenges related to routing,16,17 medium access control (MAC),18,19 transmission range,20 mobility,21 energy issues,22–24 location management,25–28 and security.29 Among all, the main issue is the failure of nodes or communication links due to instability observed in this network. Since MANET does not have any central management technique such as a terrestrial fixed wireless network, many attackers and unauthorized users can invade and attack this network easily. As we have discussed above, all nodes interact and develop trust levels for routing; therefore, attack on any node can easily disturb and destabilize the whole network. Blackhole attack is a well-known attack; it generates a fake trust level for the destination in an open MANET network. This article presents a novel and an appropriate solution to secure MANET. We have compared the performance of two existing MAC protocols in the presence of a blackhole attacker and identified the secure MAC protocol for the MANET.

**Routing issues**

MANET uses different routing protocols to establish network dynamic topology and maintain end-to-end routing information within the network. Therefore, MANET’s nodes have all routing information without
any help of fixed base stations or access points in the network. Many routing protocols have been developed with different routing techniques such as proactive, reactive, and hybrid routing techniques; these all are topology-based routing protocols, as shown in Figure 3. In proactive routing methods, the routing protocols establish all information before nodes start communication. When any node needs routes, proactive routing protocol assigns the pre-calculated shortest route. Destination-sequenced distance vector (DSDV) routing is the famous routing protocol under this category. Reactive routing protocols, in contrast, create the shortest routing path on the demand of nodes. Ad hoc on-demand distance vector (AODV) routing is a popular routing protocol under this category. Hybrid routing protocol uses the features of both proactive and reactive routing protocols such as the zone routing protocol (ZRP).

### MAC issues

MAC protocols assign the channel accessing for communication MAC protocols that do not have any routing capability. MAC protocols are designed to increase channel utilization and network lifetime, decrease delay, and safeguard the overall network. According to Noori and Ardakani, the network lifetime is the time period over which the network can operate effectively. It can also be referred as the percentage of dead nodes and as the moment when the number of live nodes drops below \((1 - \beta)N\), where \(0 \leq \beta < 1\) and \(N\) stands for the total number of nodes in the network.

The nodes in MANET use a shared channel to exchange information among nodes. Collision may occur among the transmitting nodes due to the shared channel. As a reason, MANET needs some dynamic MAC protocols that can easily avoid and handle collisions. These protocols can be typically categorized into two main groups: contention-based and schedule-based (contention-free) MAC protocols. Using contention-based protocols, a single radio channel is shared by all nodes and is allocated on demand. An example of such MAC is carrier-sense multiple access with collision avoidance (CSMA/CA) (802.11b) used in MANET. Schedule-based protocols are a class of deterministic MAC protocols in which access to the channel is based on a schedule. This is achieved based on the pre-allocation of resources to individual nodes. An example of such a scheme is time-division multiple access (TDMA). Figure 4 shows some categories of MAC protocols for MANET.

### Security issues

MANET is an open and less secure network. Different kinds of attacks can easily damage the MANET with their intelligence. Therefore, security is an essential factor for MANET. Physical, MAC, and routing layers are an essential part of MANET. Mostly, the routing layer and MAC layer are much affected due to a different type of attack. Figure 5 shows the list of different types of attacks of MANET. Recently, many researchers have focused on the security perspectives and have either proposed new protocols or improvised the existing protocols for MANET, considering different scenarios in various simulation tools. Most of the previous studies are conducted for secure mobile communication in a less dense network, with slow speed and small terrain size showing irregularities in results. In this article, we present a secure data transmission solution for non-stationary mobile nodes in MANET using MAC protocols. Our contributions are summarized as follows:

1. We have proposed a novel MAC protocol for a secure MANET scenario. For the first time, we have used preamble information to make the network more secure than the previous version of the MANET.
2. To the best of our knowledge, this is the first comparative performance analysis of contention-based and schedule-based MAC protocols under blackhole attack.
3. We have executed both MAC protocols in a mobile ad hoc wireless network and evaluated the performance in terms of packet delivery ratio (PDR), average throughput, packet loss ratio (PLR), jitter, delay, and network routing load. The results show that preamble TDMA choice of MAC protocol has any edge over the CSMA/CA choice of the MAC protocol.

This article is structured as follows: section “Related work” presents the related work to the security of MANET according to the routing and MAC layers; section “Proposed method” explains the proposed methods and problem definition, section “Experimental evaluation” describes the experiments and evaluations.
with simulation results; and the final conclusion remarks are presented in section “Conclusion.”

**Related work**

Routing and MAC layers are vulnerable to various attacks in MANET. According to security threats in MANET, researchers\textsuperscript{42–53} have proposed different solutions for MANET. We, first, classify the previous work into three subsections.

**Routing protocol**

Attacker nodes in contrast to normal nodes in the network do not cooperate to transfer data packets correctly among MANET nodes. Ali Zardari et al.\textsuperscript{42} proposed a method of dual attack detection for black- and grayhole attacks (DDBG) to detect and prevent both attackers. DDBG uses an intrusion detection system (IDS) and connected dominating set (CDS) techniques. Furthermore, DDBG creates a set of nodes using CDS. DDBG also checks the energy level of nodes since the attacker node consumes a large amount of energy as compared to the normal node. The DDBG protocol technique sends some status packet from the IDS set to check the attacker node and blacklist of attackers. Moreover, the IDS node must have a high energy level to be the trusted nodes and they broadcast the status packet to detect the attacker periodically. Gupta et al.\textsuperscript{43} proposed a reliable routing technique to prevent the attack of blackhole attackers in a MANET. They found better results using the proposed routing technique. They suggested that a little change can make it more secure than the normal AODV routing protocol.

To identify routing attacks is a very challenging task. Soni and Joshi\textsuperscript{44} compared AODV with the secure ad hoc on-demand distance vector (SAODV) routing protocol under different attack conditions such as a blackhole, route disruption attack, route invasion attack, and reply attacks. SAODV sends an encrypted message against the routing attacks. SAODV gets help using asymmetric or public key encryption to broadcast secure routing packets. This protocol uses hash chain...
and digital signature to make secure mutual header and non-mutual header fields. In these fields, all routing information is included. Due to encrypted routing messages, the attacker cannot easily understand routing packets. However, the ordinary node understands encrypted messages and sends back the digital signature to source nodes. This validates, as per authors, that SAODV is more secure than normal AODV for preventing these attacks. Alomari developed an authentication scheme for routing procedures among the nodes in the MANET. They modified the AODV routing protocol according to their authentication scheme. They used a random number, secret key, and hash function to develop an authentication scheme. The random number with a timestamp was used to protect the network nodes. The random number uses a hash function to secure a secret key and restricts the doubling and fake values. This scheme solves the synchronization problem but consumes some extra bytes for storing hash and addresses of the nodes. This protocol presented better results in terms of security and authenticity as compared to the SAODV routing protocol under blackhole attack. Singh and Singh developed a modified version of AODV known as enhanced secure trusted AODV (ESTA) for multiple and loop-free disjoint paths. ESTA is a multipath data routing protocol based on a combination of trust, authentication key, and asymmetric cryptography technique for data security. However, a slightly large delay was observed in ESTA due to multipath transmissions. Based on their NS3 simulation results, the authors concluded that the ESTA routing protocol was more secure than AODV. Raj and Swadas proposed an extension of AODV called the detection, prevention and reactive AODV (DPRAODV) routing protocol. This protocol was capable of detecting and preventing blackhole attackers in MANET with improved PDR values as compared to AODV. DPRAODV first detects and isolates the blackhole node and then sends an alarm in the form of a reply packet to neighbor nodes. Neighbor m = node updates their routing table and creates a blacklist for blackhole node which will be ignored in the future routing. Khamayshe et al. proposed two secure routing protocols (e.g. binary decision diagram AODV (BDD-AODV) and Hybrid). BDD-AODV is based on the original AODV routing protocol. The Hybrid routing protocol is a combination of BDD-AODV and multiple paths in Intermediate nodes in AODV protocol (MI-AODV) routing protocols. These protocols detect and prevent blackhole attackers in the MANET and presented better results in terms of high PDR, low PLR, and low overhead compared to the AODV and MI-AODV routing protocols. “Accurate and cognitive intrusion detection system” (ACIDS) in Sivanesh and Dhulipala fixed the threshold value based on the destination sequence number and AODV route reply (RREP) messages to identify the blackhole attackers. This protocol offered better results in terms of PDR and network throughput and from security perspectives compared to AODV.

**MAC protocols: CSMA and TDMA**

In Dasari, the real-time detection of MAC layer attacks in 802.11 has been proposed. The author focused on detecting and preventing the denial of service (DoS) attack with minimal detection delay. The author suggested that the backoff attack has a more lethal effect as compared to RTS (request to send) flooding. Guang measured the misbehavior effect of MAC for network layer performance. The author simulated two reactive routing protocols known as AODV and dynamic source routing (DSR) in the MANET with two MAC attacks (e.g. backoff manipulation and RTS data packet drop attacks). They measured the disturbance of MAC attacks to the network layer. Therefore, the routing protocols did not perform very well. Aggarwal presented a new malicious attack (TO attack [various type of attacks]). Primarily, the author concentrated on detecting and handling the selfish attack on the MAC layer and suggested detection and reply schemes. The reply depended on two stages: the first is mitigating and the second is punishing mechanisms. Both stages help improve the network performance in identifying the attacker. By their simulation results, they showed good accuracy in identifying the attacker node. Zhou and Nettles proposed a new defense mechanism against the two types of DoS attacks (single adversary attack (SAA) and colluding adversary attack (CAA)) on 802.11. SAA destroys the real traffic and creates fake traffic flow among the nodes. In this article, the author proposed a packet by the packet authentication method to control the SAA attack. To control the CAA attacks, the authors proposed more than one methods such as fair MAC protocol, introducing protecting traffic flow and adjusting distance. Gupta et al. suggested a hybrid approach to detecting sinkhole attack using the TDMA MAC protocol in the wireless sensor network (WSN). They used destination sequence number and one-hop mechanism for detecting the attacker in a network. Their approach has better efficiency in detecting the malicious node and its misbehavior. Through simulation, they showed an improvement in the results of the network using their proposed technique. They also presented an IDS for vehicular ad hoc networks (VANETs). The proposed model has the ability to detect Sybil and wormhole attacks in VANETs. They used the TDMA MAC protocol for channel access. Through the TDMA MAC protocol, they prevented the effect of attacks. The security system was more
efficient, accurate and provided quick identification of misbehavior of the attacker vehicle node in the network.

Toledo and Wang used a robust non-parametric detection mechanism for the CSMA/CA MAC protocol to prevent the DoS attack. They proposed a technique to observe the general operations of the network. They did not change existing CSMA/CA, but they only used M-truncated sequential Kolmogorov–Smirnov test to notice transmissions and the distribution of the explain-ability of collisions in MANET. The explain-ability of collision is the probability calculation of collision that describes an observation of events in the network. They observed network jamming due to DoS attacks. Due to jamming attacks, the number of collisions is increased highly in the network. They used the NS2 simulator to observe collisions due to jamming attacks. They showed that the collisions are very sensitive when the number of nodes is changing in MANET. They noticed that the explain-ability collision correctly indicated that a jammer was present in the network and nodes were not communicating correctly. Djahe et al. highlighted the MAC (802.11b) layer misbehavior for reactive (AODV) and proactive (optimized link state routing (OLSR)) routing protocols in MANET. It was found that there was no packet delivered during the virtual link attack. Using OPNET14 simulations, MAC and routing layers cooperated in the network to resist attacks and managed to achieve more throughput, PDR, and end-to-end delay in case of nodes’ misbehavior.

Secure wireless communication

Soni and Joshi implemented a combined solution for MAC and routing layers of MANET. They used cumulative frequency detection (CFD), data forwarding behavior detection (DFBD), and MAC authentication techniques to prevent the attacks on MANET. CFD uses channel busy (CB) bit with RTS/CTS (clear to send) to detect the malicious node. DFBD determines the malicious node using an incentive-based scheme. The error bit technique helps identify the malicious node in the MAC-based authentication method. This joint optimization isolated the malicious nodes efficiently and offered increased PDR and reduced PLR. An encryption method against blackhole attackers, using the Diffie–Hellman key exchange algorithm, is introduced by Taya and Gupta. Nodes use key exchange before transferring the data with the AODV routing protocol. The source node sends one key in route request (RREQ) when the source node gets RREP) from any node, it checks the critical value of RREP, and, if the key is matched with previous RREQ, then the source node starts to send data.

Dilli and Reddy used a secure hash algorithm (SH-3)-based technique called hash-based MAC–SH-3 (HMAC-SH-3) in AODV against DoS, blackhole, and cooperative blackhole attacks in MANET. They detect and prevent multiple attackers using confirmation hash-based MAC messages, secrete keys, and reliability of node. In the presence of multiple attackers, QualNet simulation revealed that the proposed algorithm improved network throughput and PDR. Ndajah et al. analyzed blackhole attackers in the peer-to-peer (P2P) wireless network. They modified the AODV routing protocol and considered the action of disobeying each node in the network. They used an active table where each node stores its identification, number of RREQ messages, and number of RREP messages. Each packet is signed using a public key of all nodes in the network. Whenever any node receives any message, it increases the sequence number of the corresponding message. Due to the digital signature and activity of each node, their proposed work is more secure than other traditional protocols. Mishra et al. presented a collective analysis of existing MAC protocols of the WSN and focused on two MAC protocols, that is, localized encryption and authentication protocol (LEAP) and TinySec, which are used for monitoring attacks in WSNs. It was observed that TinySec is lightweight but not suitable from the WSN security point of view. On the other hand, LEAP is not lightweight, but it handles attacks reasonably and makes WSN more secure.

Proposed method

Problem definition

MANET is a dynamic network, and it does not have any centralized management system. Therefore, many issues occur; the security of traffic is one of them in MANET. However, attack strategies that target the interaction between the MAC layer and the routing layer have not been fully explored. In the absence of interaction between MAC and routing layers, a new class of attacks is created. These attacks extend to the routing layer from the MAC level, where they appear as blackhole attacks, thus inflicting severe degradation over the network’s overall performance between terms concerning the carried out throughput, latency, and connectivity.

CSMA/CA (802.11b) in MANET

The traditional contention-based protocol is used for short-distance communication, which, unlike the schedule-based ones, does not require coordination between nodes getting access to the channel. Node with information to be sent must try to get bandwidth by collisions with other node transfers are minimized. If a collision occurs, the colliding nodes return for a
random period before attempting to reuse the channel. These MAC protocols are more efficient than the other MAC protocols if the nodes have burst data. CSMA is one such contention-based approach. It uses the carrier-sense multifunction to avoid collisions due to CSMA/CA shared media. In CSMA/CA, when a node needs a channel to send data, it first listens to the channel to see if another node is currently using the channel.

It performs four steps when any node needs a channel for transmitting the data: (1) listen to the favored channel; (2) if the channel is idle (no active transmitters), it sends a packet; (3) if the channel is engaged, then the node waits until the transmission quit afterwards a rivalry period where minimum age a host has to transfer before it does stay secure so the no sordid host’s piece has collided including its transmission; (4) if the duct is nevertheless idle at the stop regarding the rivalry period after the node transmits its piece in any other case that repeats the procedure described in step 3 above until it receives a broad channel. In Figure 6, the flowchart of CSMA/CA is presented.

CSMA/CA optionally utilizes RTS/CTS after the trade of the data. At first, the sender tests whether or not the medium is idle; if not, postulate so, after the distributed interframe space (DIFS) devices on time, it publicizes an RTS body to the receiver address. Second, if the grantee is inside the range, below such wish await because short interframe space (SIFS is the little day heart within the data body or its acknowledgment) one about time, after only it replied following the sender with a CTS frame. Third, the sender gets hold of the CTS frame, since it has been waiting because of every other SIFS soloist concerning era earlier than sending the statistics frame according to the receiver. Finally, so the receiver choice efficaciously obtain the facts frame, such wish pause for SIFS unit over a day or also ship an Acknowledgment (ACK) advice return following the sender.

Figure 7 shows how data are exchanged using RTS/CTS.

Due to simplicity, flexibility, and robustness, CSMA/CA is famous in wireless networks. However, the attacker attacks easily on MANETs. Therefore, the CSMA/CA protocol is less considered for secure MANET environments.

**Preamble TDMA in MANET**

In schedule-based MAC protocols, scheduling techniques settle the claims of resources (i.e. time slots)
among the MANET’s nodes. Most MANET scheduling protocols use TDMA system conversion where the channel for sending and receiving nodes is divided into different time slots. The superset of these time slots is referred to as a TDMA frame, as shown in Figure 8. In a time zone where \( N \) is a system parameter, an adjacent set of \( N \) time slots forms a logical frame that repeats periodically over time. Within each frame, each node is assigned several specific time slots.

The traditional concept of TDMA MAC was implemented in previous research\(^6\) where they used preamble information to save the energy of nodes. In this MAC protocol, the TDMA frame contains a preamble in addition to the data gaps. In the preamble, each node has its subset, sending the destination node ID of the outbound packet. The other nodes stop in the preamble and store the time slots to receive packets. Like other generic TDMA protocols (e.g. GSM), each node has a data transfer port for transferring packets. The frame structure of the preamble TDMA is shown in Figure 8, where the preamble (P) has a time duration of \( T_p \). The duration of data (\( D \)) transmission is known as \( T_d \) and the duration of guard band is known as \( T_g \). The total time duration is known as one frame time (\( T_f \)). We can say that \( T_f \) is the total time allocated for data transmission. The following equations show the mathematical calculation of all the time durations

\[
T_f = T_d + T_p + T_g
\]  
\[
T_d = T_f - N(T_p + T_g)
\]

where equations (1)–(3) represent the calculation of the length of one frame, the overall data transmission time of all nodes, and the TDMA efficiency (\( n_f \)), respectively.

The preamble TDMA MAC protocol improves transmission reliability and reduces delays in a dense network. However, in a low, dense network, the fixed frame length signifies “the lost time in the free slots” which eventually becomes slightly less. The preamble in TDMA provides a fixed slot length to all nodes including the blackhole node for time synchronization. Due to this reason, the blackhole node cannot drop all data packets of the network. Source nodes do not send all packets through the route where the blackhole attacker is present. This saves data packets. All nodes access preamble data structure for all time slots. When a node needs the channel to send and receive data, first it writes the receiving device ID into the subslot in the preamble. Following the preamble phase, each node transmits a packet in its data slot and tests the preamble to determine if the packet is being received in other time slots.

Based on a fixed schedule, the node varies between two modes of operation: active mode and sleep mode. In the active mode, the sensor wakes up and sends or receives data frames using the time slots assigned to it in a logical frame. Otherwise, they switch their transceivers off into sleep mode. The preamble-based TDMA MAC protocol is presented in Figure 9 and Table 1 and explained in the subsequent discussion.
The pseudocode of the preamble TDMA algorithm defines the data transmission time slot assigned to each node in the network for communication. First, it checks the number of active nodes \(N\); if the number of active nodes is greater than \(MaxN\), then it is not executed further because the preamble TDMA MAC protocol works on a limited number of active nodes. If the number of active nodes is within the range, then it declares the first round to \(SlotCount\). When \(SlotCount\) is in the first round, it creates a new preamble and turns on the (active mode) radio mode. A new preamble has a drop-tail queue (IFq) in which the upper layer Tx packet is stored. It runs the dequeue operation and assigned the destination node ID to \(tdmaPreamble[slot] = \text{destId}\). Then the transmitter broadcasts the packet. At the receiving address, if the radio mode is on (active), then the receiver node receives the packet and turns off the (sleep mode) radio mode; otherwise, it releases the packet.

**AODV**

AODV creates the shortest possible route with minimal end-to-end delay within the network among source and destination nodes when the source intends to communicate. This routing protocol uses some control messages (e.g. RREQ, RREP, etc.) for data transmission and reception. Initially, the source node broadcasts an RREQ message to find the path of the destination node. Either the destination node may receive directly the RREQ message or the destination receives a message via intermediate nodes. When the destination node receives the RREQ message, it unicasts the RREP message to the source node. RREP sets up a reverse path from the destination to the source node. Any intermediate node or destination node generates a route error (RRER) message due to the mobility of MANET nodes. As the source node receives RRER messages, it tries to regenerate a new route for data transmission.

**Blackhole attacker**

Blackhole attacker is one of the dangerous attackers and is aware of how to instantly retrieve a direction or path without locating the route. In each routing protocol, the source node continually communicates through the shortest and valid route with other nodes. In AODV, the shortest path and a large sequence number play a crucial role in defining a complete path. A large sequence number shows the timeliness of the path. Looking at these two parameters, the malicious node always tries to give false information that it has the shortest path with a complete large destination series number. Therefore, the source node selects the route that consists of the malicious node, ensuing in a blackhole attack that every node can misuse. It causes serious
network disruption by targeting both data and control packets, resulting in decreased network performance.

Blackhole is a lively and routed attacking method in which the attacker identifies itself as the high-quality node course for gaining access to the goal and all different nodes. In this assault, the attacker node waits till the neighboring nodes begin the RREQ packet. When an attacker node receives an RREQ message, it sends back a fake routing response (FRREP) packet with a new sequence range. Figure 10 shows a typical MANET topology of nine mobile nodes, where S is the source node, D is the destination node, node 4 is the blackhole node, and the others are intermediate nodes. S initiates broadcasting and broadcasts the RREQ message. When the RREQ message reaches the destination node D, D regenerates another message known as RREP. However, when the RREQ message arrives at node 4, an intermediate node infects it, but it regenerates a fake reply message known as FRREP with one hop count. As S receives a reply message with one hop count, then it starts to send the data packets because

### Table 1. Preamble TDMA MAC pseudocode.

| Input: |
|--------|
| $N =$ activeNodes, $Slot =$ N, $SlotCount =$ Null, $MaxN =$ 64 |
| $NothingToSend =$ $-2$, $FirstRound =$ $-1$, $Mode =$ Null, $tdmaPreamble =$ Nullarray |

| Output: Each node sends packets in a fixed time slot duration |
|--------|
| //Check the number of active Nodes |
| If ($N>$MaxN){ |
| return |
| }Else{ |
| //Deal with the preamble, cannot send anything in the first frame |
| $SlotCount =$ FirstRound |
| $tdmaPreamble[Slot] =$ NothingToSend |
| $StartSlotTimer$ |
| } |
| If ($SlotCount =$ $N$)($SlotCount =$ $FirstRound$){ |
| $Mode =$ 1 |
| //Turn on radio for the whole slot time |
| $MakePreamble()$ |
| $SlotCount =$ 0 |
| }ElseIf($tdmaPreamble[Slot] =$ NothingToSend){ |
| $Mode =$ 0 |
| //Turn off radio |
| $StartpacketTranmission$ |
| $SlotCount =$ $SlotCount + 1$ |
| } |
| $MakePreamble(){$ |
| //If IFq has pkt, assign a subslot for the destination node ID of the outgoing packet |
| If($pktTxIFq$){ |
| $tdmaPreamble[Slot] =$ destination |
| $else$ |
| $tdmaPreamble[Slot] =$ NothingToSend |
| } |
| $Recv(){$ |
| //Receiving mode |
| If(!radioActive){ |
| dopacketfree |
| //Just discard the packet |
| return |
| }Else{ |
| $Start RxPktTimer$ |
| //Will end when reception finishes |
| $Mode =$ 0 |
| //Turn off radio after receiving the whole packet |
| return |
| } |

**TDMA**: time-division multiple access; **MAC**: medium access control.

![Figure 10. MANET topology with a blackhole attacker.](image)
the source node itself does not know about any fake reply. When node 4 receives data packets, it drops all data packets instead of forwarding to the actual destination node.

The main question is “How does source node know about a fake reply message?” In TCP (transmission control protocol) connection, when the source node does not receive any acknowledge packet, the source will understand about errors but, in the UDP (user datagram protocol) connection, there is no concept of acknowledgment. Therefore, it is mostly an open problem for the UDP connection. Blackhole takes advantage of UDP connections in this article, we simulate the UDP connection in the presence of a blackhole attacker in MANET. We use AODV as a routing protocol and compare the performance of preamble TDMA and CSMA with and without blackhole attacker and verify which MAC protocol is more secure.

Experimental evaluation

Simulation setup

We have designed different MANET topologies with and without blackhole attackers to compare two different MAC protocols. For developing MANET scenarios, we have used a patch file of the blackhole attacker and implemented it in NS2. Table 2 presents the values of the simulation parameters used in the scenarios.

The attacker node moves as a standard random way mobility model that is based on pause time known as the random waypoint mobility model as we have used one blackhole attacker in our all MANET topologies. Constant bit rate (CBR) as an application and UDP as the transport protocol are used. For traffic patterns, Pascal language developed traffic generator, the following is employed. This traffic generator can create a traffic pattern in TCL format supporting end-user coding in NS2. Furthermore, we have used two different MAC protocols (CSMA and TDMA) and AODV as the routing protocol with and without a blackhole attacker. The simulated network consists of 100 randomly allocated wireless nodes in a $1200 \times 1200$ m$^2$ flat space. The random waypoint model is used for all topologies with all node mobility. Different pause mobility speeds are used, namely, 5, 10, 15, 20, 25, 30, 35, 40, 45, and 50 s. We have simulated our network scenarios according to mobility speed (m) and only one attacker is simulated to analyze the impact of a blackhole attacker in an open MANET network. Figure 11 shows the methodology of simulated scenarios.

Results and discussion

PDR (%) versus mobility speed. PDR is the ratio of the number of received data packets over the total number of the generated packet. Equation (4) is used to calculate the PDR in MANET. Results of PDR (%) versus mobility speed of nodes for TDMA and CSMA/CA (802.11b) are shown in Figure 12, considering both the presence and absence of the blackhole attacker

$$PDR(\%) = \frac{\sum RDPs}{\sum SDPs} \times 100$$ (4)

These two MAC protocols share the channel medium according to their techniques. Referring to the results, TDMA has not allocated a time slot to blackhole attacker; therefore, the attacker could not attack the network and data have been secured. On the other hand, 802.11b has allocated the same medium at the same time to all nodes of MANET. Blackhole attacks the network and keeps the channel busy. Therefore, as the mobility is increased, the attacker absorbed more data packets. CSMA does not have any alternative mechanism to control the blackhole attacker. Nevertheless, even the CSMA MAC protocol does not work well as compared to TDMA.

Normalized routing load (%) versus mobility speed. Normalized routing load (NRL) (%) is the ratio of the total generated routing packets per received data packet (RDP) to maintain the route in MANET. Equation (5) is used to calculate NRL.

$$NRL(\%) = \frac{\sum RTPs}{RDP \ at \ Destination} \times 100$$ (5)

The values of NRL (%) versus mobility speed of MANET nodes for TDMA and CSMA/CA (802.11b) are analyzed in the presence and absence of the
Figure 11. Methodology process.

Figure 12. PDR versus mobility speed in all cases.
blackhole attacker, as shown in Figure 13. Referring to the results, CSMA does not control NRL in all scenarios. Even in the absence of the blackhole attacker, NRL of MANET is high. CSMA uses a common medium at the same time and hence suffers heavily from the repeated collisions of data packets.

On the other hand, the TDMA has allocated the common channel at different time instants to all nodes and a stable link or route is maintained. As a reason, the routing protocol does not require generating a routing packet frequently due to the stability of the link, even in the case of Blackhole attacker. TDMA does not assign the channel capacity more than the fixed duration so the blackhole cannot attack the MANET anymore.

**Average delay (s) versus mobility speed.** Average delay is the difference between the total time of sent data packets (SDPs) and the total time of the received data packets (RDPs) divided by the total number of connection (cN) in the MANET. Equation (6) shows the general formula to calculate the average delay

\[
\text{Average delay (s)} = \frac{RDPs(t) - SDPs(t)}{\sum cN}
\]  

The average delay (s) of TDMA and CSMA/CA (802.11b) are compared as shown in Figure 14. The delay of TDMA is lower in the absence of blackhole than in the presence of blackhole. However, the delay is lower than that of CSMA. CSMA suffers more delay in both cases, even in the absence of blackhole when compared to TDMA.

**Throughput (kbps) versus mobility speed.** Throughput (kbps) is defined as the total amount of received data packets (RDPs) at the destination per unit time. Equation (7) shows the formula to calculate the average throughput

\[
\text{Average throughput (kbps)} = \left( \frac{\sum \text{Amount of RDPs in bytes} \times 8 \text{ bits}}{\text{Time}} \right) \times 1000
\]  

**Figure 13.** NRL (%) versus mobility speed in all cases.

**Figure 14.** Average delay (s) versus mobility speed in all cases.
Throughput versus mobility speed results shown in Figure 15 highlight that the throughput of CSMA/CA (802.11b) is less than that of TDMA. In the case of CSMA, the throughput is slightly better in the absence of blackhole. However, when the blackhole is present in the network, the throughput is very low in all mobility cases. The blackhole attacker absorbs a higher amount of data and data rarely reach the destination. On the other side, the throughput of TDMA MAC is good; as the mobility speed is increased, the throughput also increased. In the blackhole absence scenario, throughput is constant and high, whereas in its presence the throughput is not good initially, but TDMA controls the channel utilization which leads to increased throughput. Even at the last peak point, it is higher than the constant scenario.

**Figure 15.** Throughput (kbps) versus mobility speed in all cases.

**Jitter (ms) versus mobility speed.** Jitter quantifies the variation in the delay of received packets. It is measured as the sum of the difference between time of the current received data packet (\(T_{RDP}\)) and time of the previously received packet (\(T_{PRDP}\)). Equation (8) presents the calculation of jitter

\[
Jitter\ (ms) = \sum (T_{RDP} - T_{PRDP})
\]  

Figure 16 shows the result of jitter (ms) versus mobility speed. Jitter is the foremost important factor of the network. The jitter of CSMA (802.11b) is high in both cases of the blackhole. Even when the blackhole is not present, the jitter of CSMA is higher than that of TDMA. In the case of TDMA, the jitter is very low when the blackhole is not present. However, in the scenario where the blackhole is present, the jitter is increased linearly at a high mobility speed, but it is lower than that of CSMA.

**Figure 16.** Jitter (ms) versus mobility speed in all cases.

**PLR (%) versus mobility speed.** PLR (%) is the ratio of the dropped data packets (DDPs) over generated data packets (GDPs) at the source node. Equation (9) is a
general equation that is used to calculate the PLR in MANET

\[ \text{PLR} (%) = \frac{\sum DDPs}{\sum GDPs} \times 100 \] (9)

The PLR (%) values of TDMA and CSMA/CA (802.11b) are analyzed as shown in Figure 17 in the presence and absence of blackhole attacker. It shows that TDMA saves more data from the attack of blackhole because TDMA does not allocate a time slot to the blackhole attacker frequently. The loss ratio is constant without a blackhole attacker scenario. On the other hand, in the case of 802.11b, the loss ratio is higher even when there is no blackhole attacker. When the blackhole attacker is active in MANET, the loss ratio is increased. At the high mobility speed, the PLR grows to be higher and the channel remains busy as the blackhole absorbs all data. Moreover, CSMA does not have any alternative mechanism to control packet loss and prevent the blackhole attacker.

**Conclusion**

This article compares the performance of preamble TDMA and CSMA (802.11b) under blackhole attack. CSMA/CA is not capable of controlling the blackhole and there is no guarantee for successful transmission. CSMA-based protocols suffer from packet loss and extreme delays in high-density networks, whereas TDMA-based protocols work best to improve transmission reliability and suffer fewer delays in a dense network. Simulation analyses in NS2 reveal that, with a fixed slot length to all nodes including the malicious node, preamble TDMA provides improved data packet delivery and avoids/minimizes the effect of blackhole data loss. Furthermore, preamble TDMA suffers less from jitter and delay as compared to the CSMA/CA MAC network. It can be concluded that the overall performance of preamble TDMA is better than that of the CSMA/CA MAC protocol.

**Declaration of conflicting interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**Funding**

The author(s) received no financial support for the research, authorship, and/or publication of this article.

**ORCID iDs**

Kamran Ali Memon [https://orcid.org/0000-0003-1353-2586](https://orcid.org/0000-0003-1353-2586)

Imran Memon [https://orcid.org/0000-0002-9325-4805](https://orcid.org/0000-0002-9325-4805)

**References**

1. Ali K, Zhang Q, Butt RA, et al. Traffic-adaptive inter wavelength load balancing for TWDM PON. *IEEE Photonics J* 2019; 12: 7200408.
2. Mohammadani KH, Kazi H, Shaikh A, et al. A comparison of homogeneous vs heterogeneous choice of routing protocols in integrated wireless networks. *Eng Sci Technol Int Res J* 2017; 1(3): 44–50.
3. Liu X, Liu Y, Xiong NN, et al. Construction of large-scale low-cost delivery infrastructure using vehicular networks. *IEEE Access* 2018; 6: 21482–21497, [https://ieeexplore.ieee.org/document/8339515/](https://ieeexplore.ieee.org/document/8339515/)
4. Larsen E, Landmark L and Kure Ø. The effects of a UAV on a terrestrial MANET. In: *MILCOM 2018-2018 IEEE military communications conference (MILCOM)*, Los Angeles, CA, 29–31 October 2018, pp.816–821. New York: IEEE.
5. Mohammadani KH, Kazi H, Channa I, et al. A survey on integrated wireless network architectures. *Int J Comput Appl* 2013; 79: 4–9.
6. Xu X, Yang H and Kargoll B. Robust and automatic modeling of tunnel structures based on terrestrial laser
scanning measurement. Int J Distrib Sens Networks 2019; 15(11): 1550147719884886.

7. Xu X, Augello R and Yang H. The generation and validation of a CUF-based FEA model with laser-based experiments. Mech Adv Mater Struct. Epub ahead of print 18 November 2019. DOI: 10.1080/15376494.2019.1697473.

8. Priyanka Kumar S and Singh R. Performance analysis of IEEE 802.11p protocol with retry limit in VANEts: an analytical study. Procedia Comput Sci 2019; 152: 195–203, https://www.sciencedirect.com/science/article/pii/S1877050919306957

9. Shabut AM, Kaiser MS, Dahal KP, et al. A multidimensional trust evaluation model for MANETs. J Netw Comput Appl 2018; 123: 32–41. https://www.sciencedirect.com/science/article/pii/S1084804518302327

10. Khanna N and Sachdeva M. Study of trust-based mechanism and its component model in MANET: current research state, issues, and future recommendation. Int J Commun Syst 2019; 32(12): e4012, http://doi.wiley.com/10.1002/dac.4012

11. Boukerche A and De Grande RE. Vehicular cloud computing: architectures, applications, and mobility. Comput Networks 2018; 135: 171–189, https://www.sciencedirect.com/science/article/abs/pii/S1389128618300057

12. Swain J, Pattanayak BK and Pati B. Study and analysis of routing issues in MANET. In: 2017 international conference on inventive communication and computational technologies (ICICCT), Coimbatore, India, 10–11 March 2017, pp.506–509, http://ieeexplore.ieee.org/document/7975251/ (accessed 23 July 2019).

13. Goyal P, Parmar V and Rishi R. MANET: vulnerabilities, challenges, attacks, application. IJCET Int J Comput Eng Manag 2011; 11, www.IJCET.org (accessed 23 July 2019).

14. Liu X, Li Z, Yang P, et al. Information-centric mobile ad hoc networks and content routing: a survey. Ad Hoc Networks 2017; 58: 255–268, https://www.sciencedirect.com/science/article/abs/pii/S1570851616301019

15. Xu X, Yang H, Augello R, et al. Optimized free-form surface modeling of point clouds from laser-based measurement. Mech Adv Mater Struct. Epub ahead of print 10 October 2019. DOI: 10.1080/15376494.2019.1688435.

16. Desai AM and Jhaveri RH. Secure routing in mobile ad hoc networks: a predictive approach. Int J Inf Technol 2019; 11(2): 345–356, http://link.springer.com/10.1007/s41870-018-0188-y

17. Kaliappan M and Paramasivan B. Enhancing secure routing in mobile ad hoc networks using a dynamic Bayesian signallng game model. Comput Electr Eng 2015; 41: 301–313, https://www.sciencedirect.com/science/article/pii/S0045790614030979

18. Wang S-S, Li C-C, Lin H-W, et al. A passive self-configuration MAC protocol for supporting network management in IEEE 802.11-based multi-hop mobile ad hoc networks. J Netw Comput Appl 2015; 56: 149–57, https://www.sciencedirect.com/science/article/pii/S1084804515001368

19. Akhtar A and Coleri Ergen S. Directional MAC protocol for IEEE 802.11ad based wireless local area networks. Ad Hoc Networks 2018; 69: 49–64, https://www.sciencedirect.com/science/article/pii/S1570851617301816

20. Moussaoui A and Boukeream A. A survey of routing protocols based on link-stability in mobile ad hoc networks. J Netw Comput Appl 2015; 47: 1–10, https://www.sciencedirect.com/science/article/pii/S1084804514002148

21. Akbari Torkestani J and Meybodi MR. Mobility-based multicast routing algorithm for wireless mobile ad-hoc networks: a learning automata approach. Comput Commun 2010; 33(6): 721–735, https://www.sciencedirect.com/science/article/pii/S016013140900320X

22. Das SK and Tripathi S. Intelligent energy-aware efficient routing for MANET. Wirel Networks 2018; 24(4): 1139–1159, http://link.springer.com/10.1007/s11276-016-1388-7

23. Yang H and Xu X. Multi-sensor technology for B-spline modelling and deformation analysis of composite structures. Compos Struct 2019; 224: 11000.

24. Tiwari A and Kaur I. Performance evaluation of energy efficient for MANET using AODV routing protocol. In: 2017 3rd international conference on computational intelligence & communication technology (CICIT), 2017, pp.1–5, http://ieeexplore.ieee.org/doi/10.1109/CICIT.2017.7977328/

25. Sharma SB and Chauhan N. Security issues and their solutions in MANET. In: 2015 international conference on futuristic trends on computational analysis and knowledge management (ABLAZE), 2015, pp.289–294, http://ieeexplore.ieee.org/document/7155013/ (accessed 23 July 2019).

26. Sobehy A, Renault E and Muhlethaler P. Position certainty propagation: a location service for MANETs. Cham: Springer, 2019, pp.131–142, http://link.springer.com/10.1007/978-3-030-03101-5_13 (accessed 23 July 2019).

27. Rao SLA and Sunitha KVN. Position verification technique for secure geographical routing in MANET. In: 2016 thirteenth international conference on wireless and optical communications networks (WOCN), 2016, pp.1–12, http://ieeexplore.ieee.org/document/7759889/ (accessed 23 July 2019).

28. Xu X and Yang H. Network method for deformation analysis of three-dimensional point cloud with terrestrial laser scanning sensor. Int J Distrib Sens Netw 2018; 14(11): 1550147718814139.

29. Mokhtar B and Azab M. Survey on security issues in vehicular ad hoc networks. Alexandria Eng J 2015; 54(4): 1115–1126, https://www.sciencedirect.com/science/article/pii/S1110016815001246

30. Sallum EEA, dos Santos G, Alves M, et al. Performance analysis and comparison of the DSDV, AODV and OLSR routing protocols under VANEts. In: 2018 16th international conference on intelligent transportation systems telecommunications (ITST), 2018, pp.1–7, https://ieeexplore.ieee.org/document/8566825/ (accessed 23 July 2019).

31. Daas A, Molle K, Jabr E, et al. Comparison between AODV and DSDV routing protocols in mobile Ad-hoc Network (MANET). In: 5th national symposium on information technology: towards new smart world (NSITNSW), 2015, pp. 1–5, http://ieeexplore.ieee.org/document/7176394/ (accessed 23 July 2019).
32. Lv X, Le X and Ding K. An improved cluster routing algorithm based on ZRP protocol. Cham: Springer, 2017, pp. 261–271, http://link.springer.com/10.1007/978-3-319-90802-1_23 (accessed 23 July 2019).
33. Noori M and Ardakani M. Lifetime analysis of random event-driven clustered wireless sensor networks. IEEE Trans Mob Comput 2011; 10(10): 1448–1458, http://ieeexplore.ieee.org/document/5677543/.
34. Wei Ye, Heidemann J and Estrin D. An energy-efficient MAC protocol for wireless sensor networks. In: Proceedings of the 21st annual joint conference of the IEEE computer and communications societies, pp.1567–1576, http://ieeexplore.ieee.org/document/1019408/ (accessed 30 May 2019).
35. Neeraja Y and Sumalatha V. An advanced wireless medium access backoff algorithm for MANETs. In: 2015 science and information conference (SAI), 2015, pp.1033–1036, http://ieeexplore.ieee.org/document/7237269/ (accessed 23 July 2019).
36. Abbas AMH, Ali J, Rahman MA, et al. Comparative investigation on CSMA/CA-based MAC protocols for scalable networks. In: 2016 international conference on computer and communication engineering (ICCCCE), 2016, pp.428–433, http://ieeexplore.ieee.org/document/7808354/ (accessed 23 July 2019).
37. Khan S, Faisal F, Nawaz M, et al. Effect of increasing number of nodes on performance of SMAC, CSMA/CA and TDMA in MANETs. Int J Adv Comput Sci Appl 2018; 9, www.ijacsa.thesai.org (accessed 23 July 2019).
38. Jamal T and Butt SA. Malicious node analysis in MANETs. Int J Inf Technol 2019; 11: 859–867, http://link.springer.com/10.1007/s41870-018-0168-2 (accessed 23 July 2019).
39. Shahabi S, Ghazvini M and Bakhtiarian M. A modified algorithm to improve security and performance of AODV protocol against black hole attack. Wirel Netw 2016; 22(5): 1505–1511, http://link.springer.com/10.1007/s11276-015-1032-y.
40. Aggarwal R. A survey to improve the network security with less mobility and key management in MANET. Int J Sci Res Comput Sci Eng Inf Technol 2018; 3(10): 1265–1271.
41. Kaur I and Rao ALN. A framework to improve the network security with less mobility in MANET. Int J Comput Appl 2017; 167, https://pdfs.semanticscholar.org/7b42/79973d33b5f6be370c8f doll847f6b34e293.pdf (accessed 23 July 2019).
42. Ali Zardari A, He J, Zhu N, et al. A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs. Futur Internet 2019; 11(3): 61, https://www.mdpi.com/1999-5903/11/3/61.
43. Gupta P, Goel P, Varshney P, et al. Reliability factor based AODV protocol: prevention of black hole attack in MANET. Singapore: Springer, 2019, pp.271–279, http://link.springer.com/10.1007/978-981-13-2414-7_26 (accessed 29 May 2019).
44. Soni M and Joshi BK. Security assessment of SAODV protocols in mobile ad hoc networks. Singapore: Springer, 2019, pp.347–355, http://link.springer.com/10.1007/978-981-10-7641-1_30 (accessed 29 May 2019).
45. Dasari M. Real time detection of MAC layer DoS attacks in IEEE 802.11 wireless networks. In: 2017 14th IEEE annual consumer communications & networking conference (CCNC), 2017, pp.939–944, http://ieeexplore.ieee.org/document/7983259/.
46. Guang L. Vulnerability assessment of ad hoc networks to MAC layer misbehavior (Mobile CA-WC and, 2007 undefined). Wiley, https://onlinelibrary.wiley.com/doi/full/10.1002/wcm.391 (accessed 23 February 2019).
47. Guang L. Vulnerabilities of ad hoc network routing protocols to MAC misbehavior. In: IEEE international conference on wireless and mobile computing, networking and communications (WiMob 2005), 2005, https://ieeexplore.ieee.org/abstract/document/1512897/ (accessed 23 February 2019).
48. Guang L. A self-adaptive detection system for MAC misbehavior in ad hoc networks (On CA-2006 IIC, 2006 undefined), https://ieeexplore.ieee.org/abstract/document/4025045/ (accessed 23 February 2019).
49. Zhou Y and Nettles SM. Analyzing and preventing MAC-layer denial of service attacks for stock 802.11 systems, 2004, https://www.semanticscholar.org/paper/Analyzing-and-Preventing-MAC-Layer-Denial-of-For--Zhou-Nettles/89c3f7829545d942b658161c874624782781ae3b (accessed 29 May 2019).
50. Gupta D, Kaur H and Kumar R. Detection of sink hole attack in wireless sensor network using advanced secure AODV routing protocol. Int J Comput Appl 2016; 156, https://pdfs.semanticscholar.org/c962/82046f79bd0364124aeaf691297b7acef03.pdf (accessed 29 May 2019).
51. Alheeti KMA, Al-ani MS and McDonald-Maier K. A hierarchical detection method in external communication for self-driving vehicles based on TDMA. PLoS ONE 2018; 13(1): e0188760, http://dx.plos.org/10.1371/journal.pone.0188760.
52. Murugan R and Shanmugam A. A combined solution for routing and medium access control layer attacks in mobile ad hoc networks. J Comput Sci Tech 2010; 6(12): 1416–1423, http://www.thescipub.com/abstract/10.3844/jcssp.2010.1416.1423.
53. Taya M and Gupta P. A black hole detection algorithm in MANETs using MAC scheme, www.ijraset.com (accessed 29 May 2019).
54. Alomari A. Security authentication of AODV protocols in MANETs. In: International conference on network and system security, Madrid, 3–4 June 2013, pp.621–627. New York: Springer.
55. Singh D and Singh A. Enhanced secure trusted AODV (ESTA) protocol to mitigate blackhole attack in mobile ad hoc networks. Futur Internet 2015; 7(3): 342–362.
56. Raj PN and Swadas PB. DPRAODV: a dynamic learning system against blackhole attack in AODV based MANET, 2009, arXiv:0909.2371v.
57. Khamaysah Y, Yassein MB and Abu-Jazoh M. Intelligent black hole detection in mobile AdHoc networks. Int J Electr Comput Eng 2019; 9(3): 1968.
58. Sivanesh S and Dhulipala VRS. Accurate and cognitive intrusion detection system (ACIDS): a novel black hole detection mechanism in mobile ad hoc networks. Mob Networks Appl 2020, https://xs.scihub.ltd/https://doi.org/10.1007/s11036-019-01505-2.
59. Toledo AL and Wang X. Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks. *IEEE Trans Inf Forensics Secur* 2008; 3(3): 347–358.

60. Djahel S, Nait-Abdesselam F and Ahsan F. Highlighting the effects of joint MAC layer misbehavior and virtual link attack in wireless ad hoc networks. In: *2009 IEEE/ACS international conference on computer systems and applications*, Rabat, Morocco, 10–13 May 2009, pp.756–763. New York: IEEE.

61. Dilli R and Reddy PCS. Robust secure routing protocol for mobile ad hoc networks (MANETs). In: HS Saini, RK Singh, G Kumar, et al. (eds) *Innovations in electronics and communication engineering*. New York: Springer, 2019, pp.393–399.

62. Ndajah P, Matine AO and Hounkonnou MN. Black hole attack prevention in wireless peer-to-peer networks: a new strategy. *Int J Wirel Inf Networks* 2019; 26(1): 48–60.

63. Mishra B, Mohindru V and Singh Y. Comparative analysis of energy efficient secure MAC protocols for wireless sensor network. *J Basic Appl Eng Res* 2014; 1: 13–18.

64. Advanced Network Technologies Virtual Lab—IIT Kharagpur, http://vlabs.iiitkgp.ernet.in/ant/5/theory/ (accessed 16 April 2019).

65. 16.1.4.2 Preamble based TDMA protocol, https://www.isi.edu/nsnam/ns/doc/node176.html (accessed 30 May 2019).

66. Johansson P, Larsson T, Hedman N, et al. Scenario-based performance analysis of routing protocols for mobile ad-hoc networks, 1999, https://dl.acm.org/doi/pdf/10.1145/313451.313535 (accessed 23 July 2019).

67. Al-Shurman M, Yoo S-M and Park S. Black hole attack in mobile ad hoc networks. In: *Proceedings of the 42nd annual southeast regional conference (ACM-SE 42)*, 2004, p.96. New York: ACM Press, http://portal.acm.org/citation.cfm?doid=986537.986560 (accessed 23 July 2019).

68. Blackhole Patch in NS-2, http://mohittahiliani.blogspot.com/2014/05/blackhole-attack-in-ns-2.html (accessed 23 July 2019).

69. ns2.35, https://sourceforge.net/projects/nsnam/ (accessed 23 July 2019).

70. NS2 Traffic Generator, https://github.com/khalid-mohammadani/NS2