Chapter 3

Protocol for Multiple Black Hole Attack Avoidance in Mobile Ad Hoc Networks

Rushdi A. Hamamreh

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.73310

Abstract

Mobile ad hoc networks (MANETs) form a new wireless networking paradigm with unique characteristics that give them appreciated interest in a vast range of applications. However, many challenges are facing MANETs including security, routing, transmission range, and dynamically changing topology with high node mobility. Security is considered as the main obstacle for the widespread adoption of MANET applications. Black hole attack is a type of DoS attack that can disrupt the services of the network layer. It has the worst malicious impact on network performance as the number of malicious nodes increases. Several mechanisms and protocols have been proposed to detect and mitigate its effects using different strategies. However, many of these solutions impose more overhead and increase the average end-to-end delay. This chapter proposes an enhanced and modified protocol called "Enhanced RID-AODV," based on a preceding mechanism: RID-AODV. The proposed enhancement is based on creating dynamic blacklists for each node in the network. Each node, according to criteria, depends on the number of mismatches of hash values of received packets as compared with some threshold values, and the sudden change in the round-trip time (RTT) can decide to add or remove other nodes to or from its blacklist. The threshold is a function of mobility (variable threshold) to cancel the effect of normal link failure. Enhanced RID-AODV was implemented in ns-2 simulator and compared with three previous solutions for mitigating multiple black hole attacks in terms of performance metrics. The results show an increase in throughput and packet delivery ratio and a decrease in end-to-end delay and overhead ratio.

Keywords: enhanced RID-AODV, MANET security, multiple black hole attacks, network layer attack

1. Introduction

A mobile ad hoc network (MANET) is a network of mobile nodes that are able to move arbitrarily and are connected by wireless links. It is a self-configuring network that does

not require any preexistent infrastructure such as centralized management or base stations. If two mobile nodes are within each other transmission range, then they can communicate with each other directly; otherwise, the nodes in between have to forward the packet for them. Hence, mobile nodes are not only functioning as hosts but they are also functioning as routers [1, 2].

Because MANETs are infrastructure-less networks with no centralized administration, they can be self-deployed in a short time. The easy deployment of nodes, self-organizing nature, and freedom of mobility make MANETs suitable for a broad range of applications. They can be useful in disaster recovery and emergency operations where there is not enough time or resources to install and configure an infrastructure. They are also used in other applications, for example, in military services, maritime communications, vehicle networks, casual meetings, campus networks, robot networks, etc., [3].

On the other hand, MANETs are vulnerable to various attacks at all layers. So, much research has been conducted on providing security services for MANETs, because security is the main obstacle for the widespread adoption of MANET applications. MANETs are vulnerable in their functionality: intruders can compromise the operation of the network by attacking at any of the physical, MAC, or network layers. The network layer, especially the routing protocol, is vulnerable because of the use of cooperative routing algorithms, the limited computational ability of nodes, the exhaustible node batteries, the lack of clearly defined physical network boundary, and the transient nature of services in the network. Standard information security measures such as encryption and authentication do not provide complete protection; thus intrusion detection and prevention (IDP) mechanisms are widely used to secure MANETs [4].

Attacks in MANET can be divided, according to the criteria that whether they disrupt the operation of a routing protocol or not, into two classes: passive attacks and active attacks. In passive attacks, the attacker attempts to discover valuable information but does not disrupt the operation of the routing protocol. Active attacks, however, involve actions like modification and deletion of exchanging data to absorb packets destined to other nodes to the attacker for analyzing or disabling the network [5].

Black hole attack is a type of active attack that exploits the route reply message (RREP) feature of the routing protocol. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. A RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any other RREP messages from other neighboring nodes or even from the actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them [6].

So, the black hole attack is a DoS attack that disrupts the services of routing layer by exploiting the route discovery process of AODV. According to many research studies that focus on studying the effects of malicious attacks on network performance, the simulation results show that the black hole attack is more dangerous than other attacks in the network layer [7].

http://dx.doi.org/10.5772/intechopen.73310

Several mechanisms and protocols have been proposed to detect and mitigate its effect using different strategies. However, many of these solutions impose more overhead and increase the average end-to-end delay. In this paper, we propose a modified and enhanced protocol that aims to detect and mitigate the effects of multiple black hole attacks in MANETs. The proposed solution, "Enhanced RID-AODV," was implemented in ns-2 simulator and compared with three previous solutions for mitigating multiple black hole attacks in terms of performance metrics. The results show an increase in throughput and packet delivery ratio and a decrease in end-to-end delay and overhead ratio.

The rest of this paper is organized as follows: Section 2 provides some details about the black hole attack; Section 3 provides the related work in detection and mitigation of black hole attack. The proposed protocol is introduced in Section 4; the simulation and network environment is described in Sections 5 and 6, the analysis and the results are discussed. Finally, the conclusion is presented in Section 7.

2. Black hole attack in MANETs

Routing protocols in mobile ad hoc networks by their nature are distributed routing protocols with the assumption that all nodes in the network will cooperate truly and participate honestly. However, the existence of malicious nodes makes this assumption not true. Such nodes may drop the packets, if they are not the destination, without forwarding them or may disrupt the routing discovery and maintenance processes resulting in abnormal network operation that affects the performance of the network and may cause denial of service [8].

A black hole attack is a kind of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them (drop all packets) without forwarding them to the destination [9].

In reactive routing protocols such as AODV, the destination sequence number (*dest_seq*) is used to describe the freshness of the route. A higher value of *dest_seq* means a fresher route. On receiving a RREQ, an intruder can advertise itself as having the fresher route by sending a route reply (RREP) packet with a new *dest_seq* number larger than the current *dest_seq*

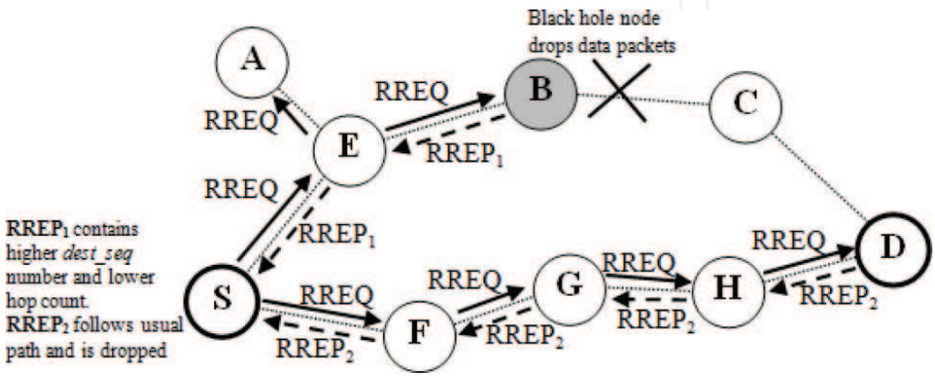

Figure 1. Black hole attack illustration.

number. In this way the intruder becomes part of the route to that destination [10]. **Figure 1** illustrates the black hole attack where nodes S and D are the source and destination, respectively, and node B is the black hole.

A black hole has two properties: First, the node exploits the ad hoc routing protocol to advertise itself as having a valid route to a destination, even though the route is spurious with the intention of intercepting packets. Second, the node consumes the intercepted packets. In an ad hoc network that uses the AODV protocol, a black hole node absorbs the network traffic and drops all packets [9].

3. Materials and methods

Several mechanisms and protocols using different strategies have been proposed to protect MANETs against black hole attacks. In addition, some research studies have focused on studying the effect of malicious nodes on network performance without providing any solutions. Kanthe et al. studied the effect of malicious attacks in mobile ad hoc networks including black hole attack, packet drop attack, and gray hole attack on AODV protocol under different performance metrics: throughput, packet drop rate, and end-to-end delay. It was found that the black hole attack is more dangerous than other attacks mentioned in this paper [7].

Aad et al. provided a quantitative study of the performance impact and scalability of DoS attacks in ad hoc networks. They have also considered the black hole attack, as its impact in ad hoc networks. The authors considered the following as critical performance measures for a system under attack: total system throughput and probability of interception in addition to the system fairness measures and the mean number of hops for a received packet. The simulation results for the impact of black hole node showed that the system has high fairness index with no black hole in the network [11].

Dinesh Mishra et al. analyzed the effects of black hole attack in mobile ad hoc network using AODV and DSR routing protocols. The authors considered the throughput as the main performance measure. Simulation results, by NS-2 simulator, showed that a higher data packet loss when using DSR as compared to AODV. The observation and results showed that DSR data loss is around 55–60% in the presence of black hole attack, while 45–50% in the AODV routing. AODV protocol provides better performance than the DSR in the presence of black holes with minimal additional delay and overhead [12].

Sonja Buchegger and Jean-Yves Le Boudec proposed a robust reputation system for misbehavior detection in mobile ad hoc networks. Nodes have a monitor for observations, reputation records for first-hand and trusted second-hand observations about routing and forwarding behavior of other nodes, trust records to control trust given to received warnings, and a path manager to adapt their behavior according to reputation and to take action against misbehaved nodes. Nodes monitor their neighbors and change the reputation accordingly. When the reputation rating is bad, they take action in routing and forwarding. The routes

containing the misbehaved node are either reranked or deleted from the path cache. In addition, once a node has detected a misbehaved node, it informs other nodes by sending an ALARM message [13].

Deng et al. proposed a method to solve the black hole problem. This method is to disable the ability of an intermediate node to reply in a RREP message, so all reply messages should be sent out only by the destination node. This method increases the routing delay, especially for a large network. Besides, a malicious node can take advantage by fabricating a reply message claiming it was sent from the destination node. Another solution was proposed in this paper that depends on using one more route to the intermediate node that replays the RREQ message to check whether the route from the intermediate node to the destination node exists or not. If it does not exist, the reply message from the intermediate node is discarded and an alarm message to the network is sent out. Using this method, the black hole problem was avoided, and further malicious behavior was also prevented. This method cannot prevent multiple black hole attacks [14].

Seungjoon Lee et al. proposed a method to avoid black hole attack based on introducing additional route confirmation messages: route confirmation request (CREQ) and route confirmation reply (CREP). In the proposed method, the intermediate node requests its next hop to send a confirmation message to the source. After receiving both route reply and confirmation message, the source determines the validity of path according to its policy. Simulation results show remarkable improvement in 30% higher delivery ratio. Its drawback is that it cannot detect multiple black hole attacks and the control messages have been increased [15].

Kurosawa et al. proposed an anomaly detection scheme for black hole nodes using dynamic training method in which the training data is updated at regular time intervals. They considered the destination sequence number in order to detect this attack. In normal state, sequence number changes depending on its traffic conditions, and the destination sequence number tends to rise monotonically when the number of connections increases. However, during the attack, the sequence number is increased largely. A statistical method is applied for detection of black hole that is based on the difference between destination sequence numbers of received RREPs. The simulation results of this method showed significant effectiveness in detecting the black hole attack as compared with conventional scheme. Through the simulation, our method shows significant effectiveness in detecting the black hole attack [16].

The solution proposed by Kumar and Selvakumar, focuses on the requirement of a source node to wait unless there is arrival of RREP packet from more than two nodes. When it receives multiple RREPs, the source node checks that there is any share hops or not. The source node will consider the route safe if it finds the share hops. Its drawback is the introduction of time delay it has to wait for the arrival of multiple RREPs before it judges the authentication of node [17].

A lightweight routing protocol IDSAODV was proposed by Dokurer et al. in [18] as a solution for black hole attack problem in MANETs. The authors manually analyzed the output file obtained from simulation and found out very soon after the first RREP from the destination node a second RREP arrived at the source node. Through simulation, they found out that the

first RREP was from the black hole node and the second RREP was from the intended destination. At this point, for future simulations, they assumed that the first RREP would always be from black hole node and modified the AODV protocol to ignore the first RREP and send using second RREP route. A RREP caching mechanism to count the second RREP message was added to aodv.cc file in NS-2 [18].

The simulation results demonstrate that IDSAODV improved the PDR in a MANET with a single black hole node, thus proving the successful implementation of the route caching mechanism [18].

Many of the proposed solutions that make the route establishment process longer while the nodes are moving are facing from the link failure problem. Shree and Ogwu in [6] addressed this issue by getting advantage of the reverse AODV (RAODV) routing protocol proposed by Kim et al. in [19]. RAODV discovers route using reverse route discovery procedure where the destination node sends reverse-route request (R-RREQ) messages to its neighbors to find a valid route to the source node after receiving RREQ from source node. Their simulation results of RAODV show that it does improve the performance of AODV in metrics such as packet delivery ratio (PDR), end-to-end delay, and energy consumption [6, 19].

Although RAODV has not been designed to prevent black hole attacks and it was developed with the aim of solving path failure problem, Shree and Ogwu proposed in [6] to use it in mitigating the effects of black hole attacks in ad hoc networks. Therefore, they proposed RID-AODV protocol that combines RAODV (proposed in [19]) and IDSAODV (proposed in [18]) to withstand multiple black hole attacks in client-based WMNs [6].

4. The proposed protocol: enhanced RID-AODV

Routing is an essential operation in all network types, and it has special importance in ad hoc networks, because in such networks, nodes are operating not only as hosts, but they are also operating as routers. Therefore, any breakthrough in the routing process has a direct impact to the performance of the whole network. This is the reason why routing is targeted in many kinds of attacks in MANETs especially black hole attack.

The proposed protocol, "Enhanced RID-AODV," is a modification and enhancement of the RID-AODV protocol proposed in [6]. RID-AODV protocol was proposed as combination of previous two protocols, namely, IDSAODV (which is proposed in [18]) and RAODV (proposed in [19]) as mentioned in the previous section. Therefore, we got all the advantages of the preceding protocols in mitigating the bad impact of the existence of malicious black hole nodes in the ad hoc network. Thus, better results in terms of performance metrics [20].

The detection of the malicious nodes and mitigation their effects can be achieved by creating and maintaining *dynamic blacklist* in each node according to some criteria. Then each non-malicious node will prevent sending or forwarding to the neighboring nodes that exist in its own blacklist either in the forward or reverse path. In other words, each node will not use blacklisted nodes as intermediate nodes. Dynamic blacklist means that each node adds and

removes nodes to or from its blacklist automatically according to specific criteria as will be explained in this section.

The criteria for each node to add another node's address in its blacklist is the repetitive mismatch in the hash value of the receiving frames (layer 2 frame) from the same neighboring node. So, each node keeps a counter for each other node that receives a frame from the neighboring nodes. If there is a mismatch between the received hash value and the calculated value, the corresponding counter for the sending (or forwarding) node will be incremented. When the counter reaches some threshold value (*malPcktThreshold*), then the corresponding neighboring node will be blacklisted [21].

Each node keeps small number of counters. If node n_i has p neighboring nodes (p is $\subseteq$ of all nodes) and n_i is receiving from q nodes ($qis \subseteq ofp$), then n_i will keep only q counters for this purpose.

In addition, we can get another advantage of the nature of the reverse route discovery procedure in RAODV to create *full path* (*bidirectional*) *integrity check implemented in hop-by-hop basis* to detect any modifications on the traversing packets and to detect the causing nodes.

To distinguish between hash value mismatch that may occur as a result of normal link failure, which is from the nature of MANETs due to mobility of nodes that communicate wirelessly or from the existence of malicious nodes, the threshold value *malPcktThreshold* should be considered as a function of mobility (variable threshold). If the node is moving with relatively high speed, the mismatch of hash values is most likely due to normal link failure, and so the threshold should be high. On the other hand, if there are many hash value mismatches while the node is moving slowly, there is most likely a malicious node. So, the value of *malPcktThreshold* is directly proportional to the node speed, and it was implemented by using Eq. (1):

$$malPcktThreshold = NodeSpeed + C \tag{1}$$

where C is the threshold value when the node speed is zero.

The malicious node may not act as a black hole all the time; it may become benign for some period of time; then it may (or may not) resume its malicious activities. So, when a node adds another node's address to its blacklist, the blacklisted node will not stay in its blacklist forever. However, it will be blacklisted for a previously specified period of time. So, when a node is added to another node's blacklist, not only the address of the blacklist is added but also the expiry time for that node to be released from that blacklist. The blacklisted node expiry time is computed using Eq. (2):

$$blkListedNodeExpTime = CURRENT_{TIME} + blockingPeriod \tag{2}$$

Each time the node wants to send (or forward) a packet to a neighboring node, it will check if it is blacklisted, and if so it will also check the expiry time for that node. If it's expired, it will be removed from the blacklist of that node, and its corresponding counter and expiry timer will be reset. Because of that it is a dynamic blacklist.

When a node wants to send (or forward) a packet, in either the forward path or reverse path, it will check the routing table to decide what is the next hop. Then it will check if the next hop is blacklisted or not; if it's blacklisted, it will check the blacklist expiry time. If the next hop node is still blacklisted, then the node will remove that node from its neighbor list and run the handle link failure procedure. Then the node will try to send (or forward) the packet by using another path.

As a result, we can get a secure path that avoids the black hole malicious nodes during routing packet as shown in **Figure 2**.

The criterion for the reverse path is the round-trip time (RTT). RTT is the length of time it takes the RREQ to be sent (or forwarded) plus the length of time it takes for the R-RREQ to be received by the node. As we assumed that all the nodes are trusted, we can measure RTT in the normal behavior and use it as a reference. Any change in this value indicates that the reply was not from the original destination, so this value can be used to detect the malicious node.

The node will first measure round-trip time (RTT). Then it will calculate the average hop-to-hop time (T_{h-h}) using Eq. (3):

$$T_{h-h} = \frac{RTT}{2 * hopcount} \tag{3}$$

Now, the New RTT (RTT_{next}) should satisfy the following condition:

$$RTT - \frac{T_{h-h}}{2} < RTT_{next} < RTT + \frac{T_{h-h}}{2} \tag{4}$$

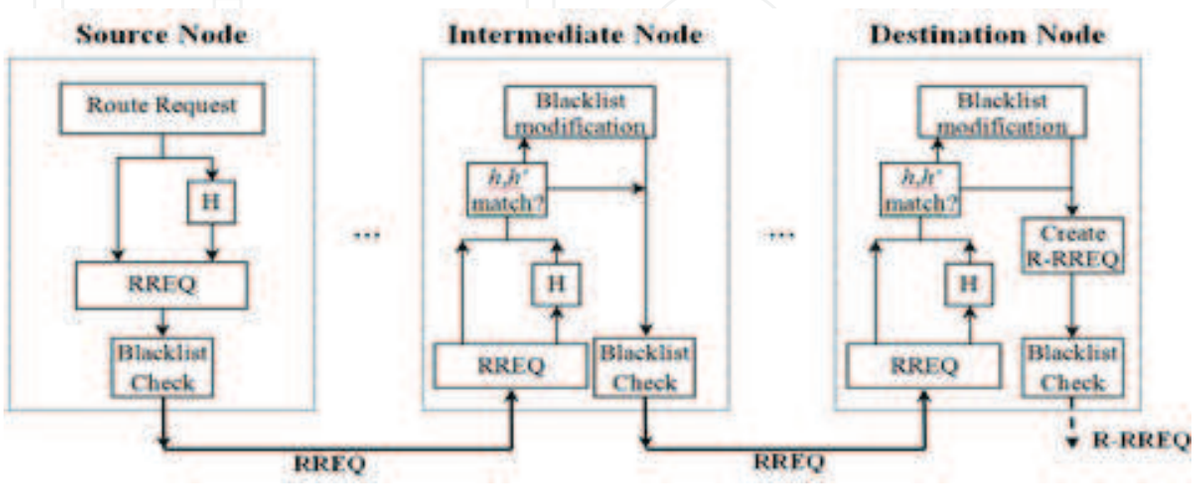

Figure 2. Secure routing path.

The sequence diagram of the Enhanced RID-AODV protocol is shown in **Figure 3**. *RTT* values are shown in normal behavior and in malicious behavior.

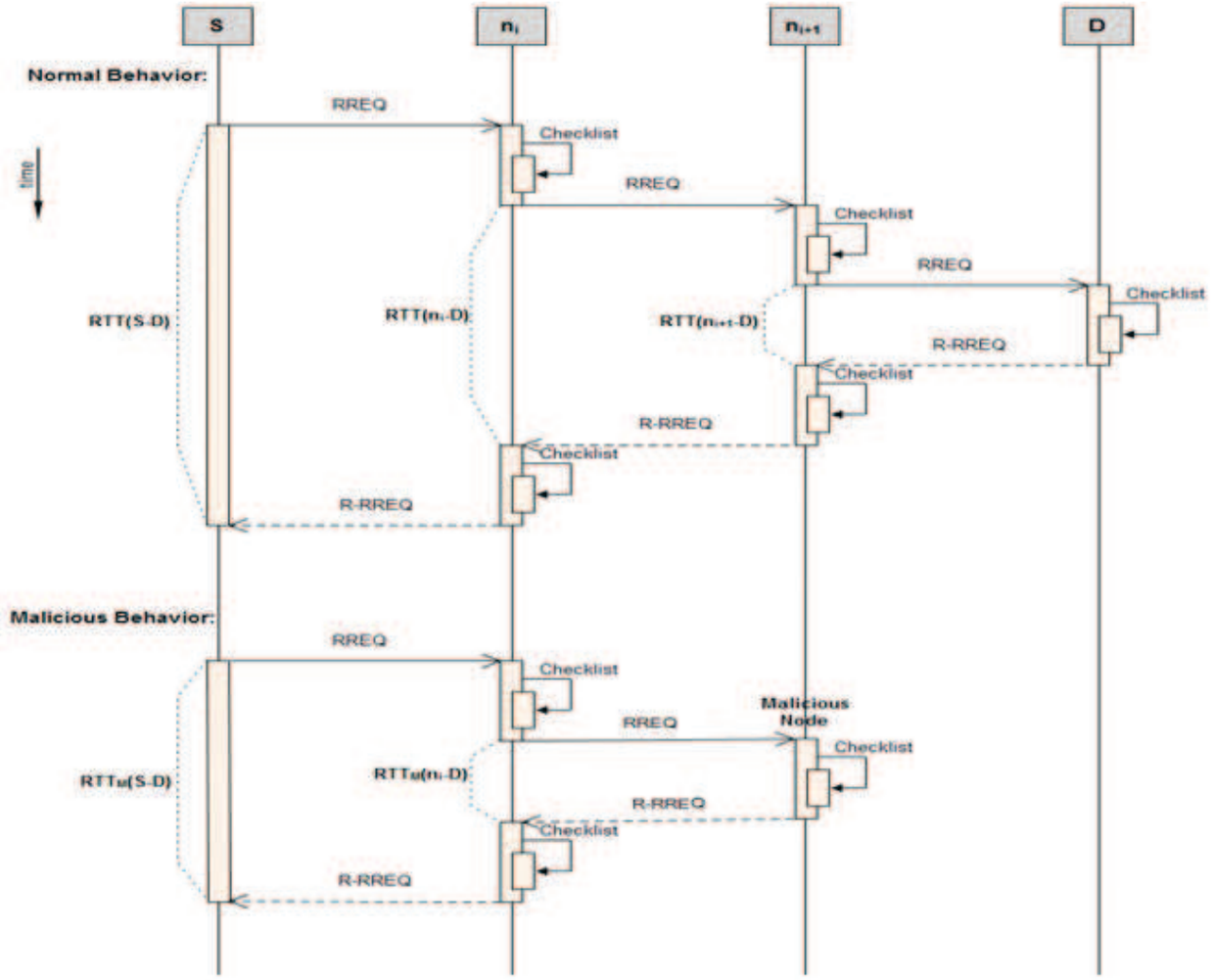

Figure 3. Sequence diagram for the Enhanced RID-AODV.

Pseudocode for the proposed protocol: How the node decides to add or remove other nodes in its blacklist:

1. Generate new hash value ($NewHash$).
2. Compare the generated hash value New_{Hash} with the received hash value with the packet $HashVal$.
3. if($NewHash \neq HashVal$ then, $incrmalNodeCouter(PrevHopAddr)$
4. Check the speed of the node ($NodeSpeed$).
5. Compute the threshold that will be used to consider a node as blacklisted $malPcktThreshold = NodeSpeed + C$
6. *//To add a node to a blacklist*
   if $(isBlacklisted(NextHop) = FALSE \wedge malNodeCouter(NextHop) > malPcktThreshold)$
   then,
   a. $addBlackList(NextHop)$.
   b. $blkListedNodeExpTime(NextHop) = CURRENT_{TIME} + BlockingPeriod$

Figure 4. Pseudocode for the proposed protocol: how the node decides to add other nodes in its blacklist.

Pseudocode for the proposed protocol: How the node decides to add or remove other nodes in its blacklist:

//To remove a node from a blacklist

if $\left(isBlaklisted\left(NextHop\right)=TRUE \wedge CURRENT_{TIME} > BlkListedNodeExpTime\left(NextHop\right)\right)$

then,

a. $removeBlackList\left(NextHop\right)$.
b. $malNodeCouter\left(NextHop\right)=0$
c. $blkListedNodeExpTime\left(NextHop\right)=0$

Figure 5. Pseudocode for the proposed protocol: how the node decides to remove a node from its blacklist.

Pseudocode for the proposed protocol: How the node behaves when sending or forwarding a packet:

if($isBlacklisted\left(NextHop\right)=TRUE$

then,

// Generate route error message

sendRERR

Figure 6. Pseudocode for the proposed protocol: how the node behaves when sending or forwarding a packet.

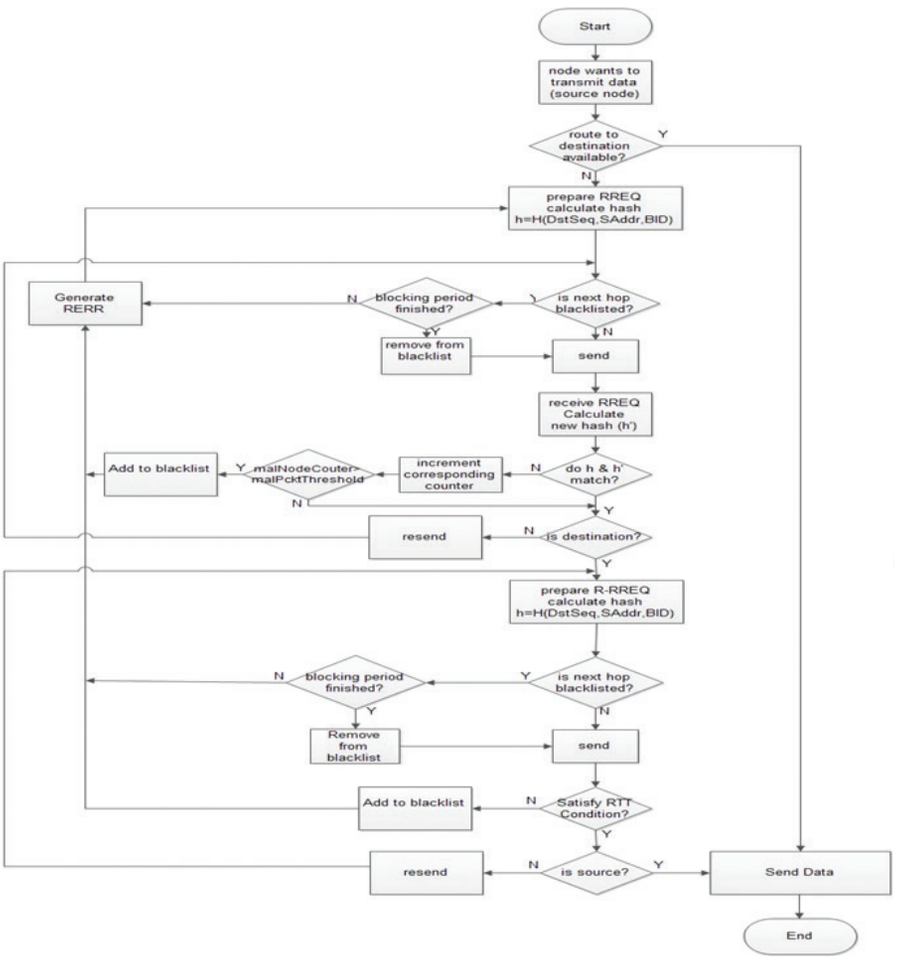

Figure 7. Flowchart of the Enhanced RID-AODV protocol.

In our protocol we used one-way hashing function on the level of packets in the routing discovery control messages. The purpose of using a hash function is to produce a "fingerprint" of the message. This fingerprint will be used for route request (RREQ) *packet authentication* and *integrity check* in each hop while traversing from source node to the destination node and for reverse route request (R-RREQ) from destination to source, resulting in a two-way (bidirectional) control packet authentication and integrity check. To implement the Enhanced RID-AODV protocol, a new field was added in the route request (RREQ) and reverse route request (R-RREQ).

The pseudocodes for the Enhanced RID-AODV protocol are presented in **Figures 4–6**.

The flowchart for the Enhanced RID-AODV protocol is illustrated in **Figure 7**.

5. Simulation and network environment

Network Simulator version 2 (NS-2) was adopted in this research study because it is one of the most popular network simulators that are appropriate to simulate the wireless networks. Ns-2 is an open-source discrete event-driven simulator that is written in C++ language. During the simulation the packet header (*aodv_packet.h* file) of the AODV route request and route reply (changed to route reverse request) is modified to hold the hash value ($Hash_{Val}$) with packet. In addition to that, the files *aodv.h* and *aodv.cc* were modified to implement the Enhanced RID-AODV protocol together with previous protocols. Also, files/*common/node.h* and */common/node.cc* have been modified to hold the q counters and the blacklists inside each node. Simulation was carried out by referring to many resources including but not limited to references [22–24].

The simulation area is a square field of 1000 × 1000 m with fixed sender and receiver nodes that communicate using intermediate mobile nodes, which are moving randomly during simulation time (these random movements were generated using *setdest* tool), and the intermediate nodes are sending random traffic pattern among each other (created using *cbrgen.tcl* command). The sender and receiver were placed in points (200,200) and (800,800), respectively. So they are out of the transmission range of each other, and all traffic between them is through the moving intermediate nodes. The parameter considered in this simulation is given in **Table 1**.

In this research, the Enhanced RID-AODV protocol together with four preceding protocols was implemented and simulated with the same environment parameters to be able to make a comparison among them. That includes the genuine AODV protocol with simulation of black hole malicious nodes, the IDSAODV protocol, RAODV protocol, RID-AODV protocol, and our proposed protocol which is Enhanced RID-AODV. For each protocol many scenarios were generated to simulate the existence of different numbers of malicious nodes in order to study the effect of multiple malicious nodes on network performance and the effectiveness of each protocol to compare among these protocols; we made as many combinations of nodes to act as malicious nodes, and then we computed the average of the results.

Parameter	Value
Simulator	ns-2
Routing protocol	AODV, IDSAODV, R-AODV, RID-AODV, Enhanced RID-AODV
Simulation time	100 sec
Simulation area	1000 × 1000 m
Number of nodes	40
Number of malicious nodes	0, 1, 2, 3, 4, 5, 6, 7
Sender node	Fixed at point (200,200)
Receiver node	Fixed at point (800,800)
Intermediate nodes	Moving randomly
Maximum speed of mobile nodes	40 m/s
Data rate	50 Kb/s
Pause time	0 sec
Transport type	UDP, CBR
Data packet size	Default
MAC protocol	IEEE 802.11

Table 1. Parameters used in simulation.

5.1. Performance metrics

Four performance metrics were considered and computed as the average of many cases in all scenarios of multiple malicious nodes for all the protocols in this research. Four separate scripts were generated to compute these performance metrics using *awk* command:

- **Throughput**: the amount of data transferred over the period of time expressed in kilobits per second (kbps). Throughput has been calculated using Eq. (5):

$$Throughput = \frac{\sum ReceivedDataPackets}{SimulationTime} \tag{5}$$

- **Packet delivery ratio (PDR)**: the percentage ratio of the total number of data packets received by the destination node to the number of data packets sent by the source node as in Eq. (6):

$$PDR = \frac{\sum NumberofReceivedDataPackets}{\sum NumberofSentDataPackets} * 100 \tag{6}$$

- **Average end-to-end delay**: the average delay between the sending of the data packet by the source node and its receipt at the destination node. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc. The average end-to-end delay was computed using Eq. (7):

$$Avg_{E2E_{Delay}} = \frac{\sum_{i=1}^{n}(ReceiveTimeofP_i - SentTimeofP_i)}{NumberofReceivedPacket} \quad (7)$$

where i is the packet index and n the last packet in the message.

- **Overhead ratio**: the ratio of the total number of control packets sent at the routing level and the total number of packets sent from the source node as in Eq. (8):

$$OverheadRatio = 1 - \frac{NumberofDataPacketsSentatRTR}{NumberofAllPacketsSentatRTR} \quad (8)$$

6. Results and analysis

Figure 8 shows the results of the throughput for the case of the existence of black hole nodes (as the number of black hole nodes increases up to seven malicious nodes) for the genuine AODV and the four solutions: IDSAODV, R-AODV, RIS-AODV, and Enhanced RID-AODV.

Figure 8 shows the effects of increasing the number of malicious nodes in the network on the throughput are clear. One black hole in the network has a huge impact in decreasing the throughput, and few numbers of malicious nodes are able to prevent all traffic from reaching the destination. Previous protocols provide sole improvements on the throughput; however, the Enhanced RID-AODV protocol provides more improvement to throughput that takes advantages from its enhancements and from the preceding protocols in stability and robustness in avoiding multiple black hole nodes.

The packet delivery ratio (PDR) was computed; the results are shown in **Figure 9**.

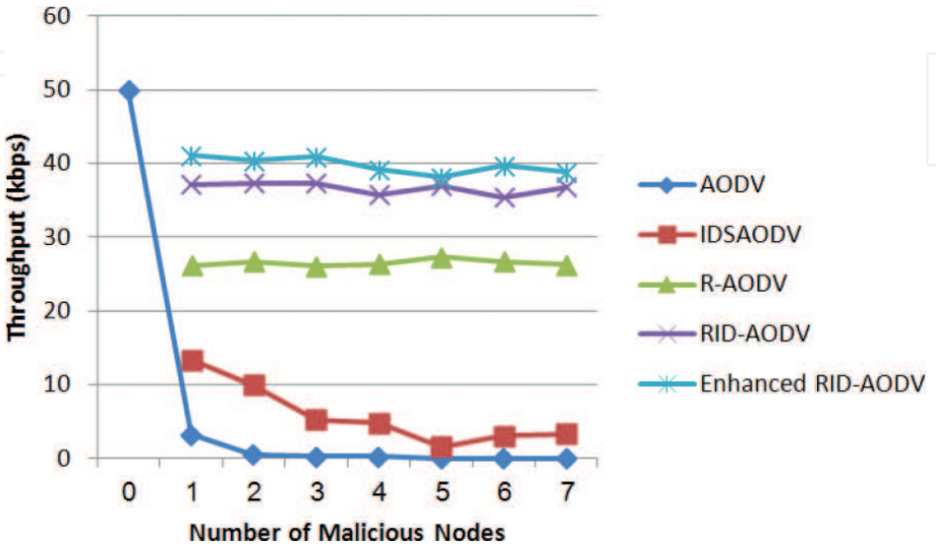

Figure 8. Throughput vs. number of malicious nodes for different protocols.

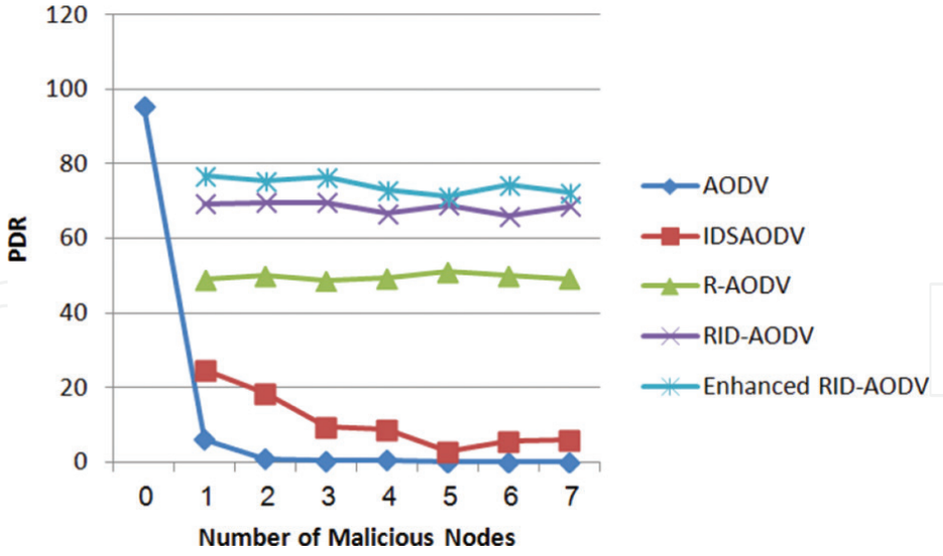

Figure 9. PDR vs. number of malicious nodes for different protocols.

The impact of malicious nodes in dropping the packets to reduce the received packets is obvious. Only one black hole node in the network is able to reduce the PDR to around 10% of the original PDR. We can notice the improvements provided by the different protocols in the research.

One of the major improvements of the Enhanced RID-AODV is decreasing the average end-to-end delay. The results are illustrated in **Figure 10**.

The previous protocols had an impact in increasing the average end-to-end delay with the increase in the throughput and PDR. However, in the Enhanced RID-AODV, due to the use of blacklists, the nodes choose the optimized path. As a result the average end-to-end delay has decreased as compared to RID-AODV. This is an important improvement because time is a significant factor in ad hoc networks.

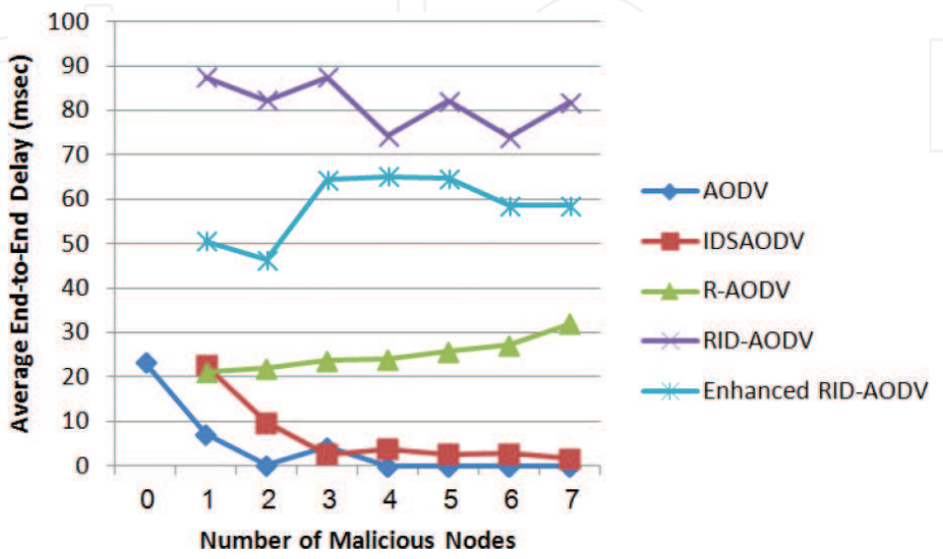

Figure 10. Average end-to-end delay vs. number of malicious nodes for different protocols.

http://dx.doi.org/10.5772/intechopen.73310

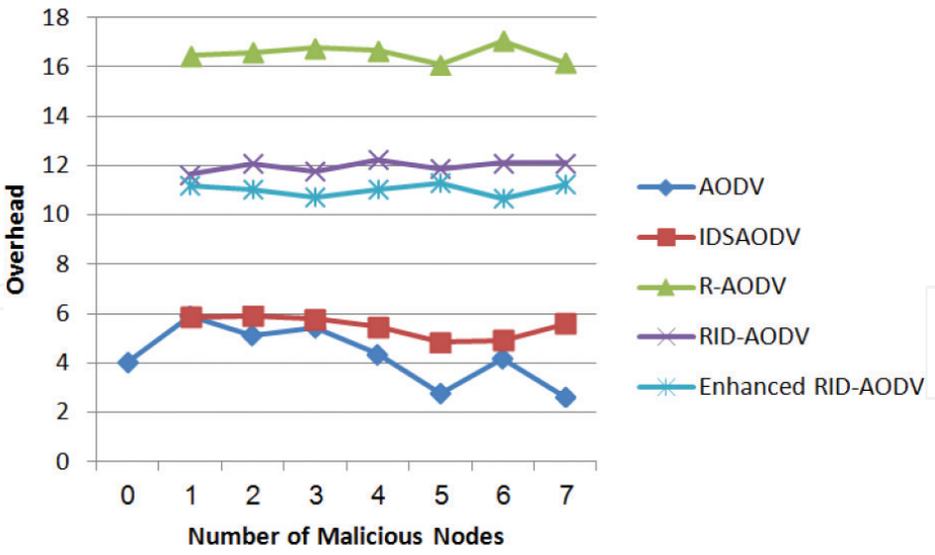

Figure 11. Overhead ratio vs. number of malicious nodes for different protocols.

Also the overhead ratio has been improved by the proposed protocol as shown in **Figure 11**.

The previous protocols impose more overhead. The increase of the overhead ratio is mainly due to R-RREQ control message. However, in Enhanced RID-AODV, and as a result of applying blacklists in the intermediate nodes, the overhead ratio has decreased.

7. Conclusion

Several mechanisms and protocols have been proposed to detect and mitigate the effects of multiple black hole attack using different strategies. However, many of these solutions impose more overhead and increase the average end-to-end delay. In this paper a new mechanism, called "Enhanced RID-AODV," was proposed to detect and mitigate the effects of multiple black hole attacks in MANETs aiming to increase the throughput and PDR while decreasing the average end-to-end delay and overhead. It is an enhanced and modified version of a previously proposed mechanism called RID-AODV. RID-AODV is a combination of two other protocols: RAODV and IDSAODV.

According to the simulation results, Enhanced RID-AODV provides higher throughput and higher packet delivery ratio than its preceding version. Also, the dynamic blacklists provide positive effects in decreasing the overhead ratio and the end-to-end delay.

Author details

Rushdi A. Hamamreh

Address all correspondence to: rhamamreh@eng.alquds.edu

Computer Engineering Department, Al-Quds University, Israel

References

[1] Corson S, Macker J. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC: 2501, IETF. [Online]. Available: http://tools.ietf.org/html/rfc2501

[2] Bakshi A, Sharma AK, Mishra A. Significance of mobile AD-HOC networks (MANETS). International Journal of Innovative Technology and Exploring Engineering (IJITEE). March 2013;**2**(4). ISSN: 2278-3075

[3] Kannhavong B, Nakayama H, Nemoto Y, Kato N, Jamalipour A. A survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications. October 2007; **14**(5):85-91

[4] Nadeem A, Howarth MP. A survey of MANET Intrusion Detection & Prevention Approaches for network layer attacks. IEEE Communications Surveys & Tutorials. 2013

[5] Behzad S, Jamali S. A survey over black hole attack detection in mobile ad hoc network. International Journal of Computer Science and Network Security (IJCSNS). March 2015;**15**(3)

[6] Shree O, Ogwu FJ. A proposal for mitigating multiple black-hole attack in wireless mesh networks. Wireless Sensor Network. 2013;**5**(4):76-83

[7] Kanthe A, Simunic D, Prasad R. Effects of Malicious Attacks in Mobile Ad-hoc Networks. IEEE International Conference on Computational Intelligence and Computing Research, ISBN:978-1-4673-2481-6,18-20, December 2012, Coimbatore, India; 2012

[8] Ehsan H, Khan FA. Malicious AODV. Implementation and Analysis of Routing Attacks in MANETs. 11th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE. 2012

[9] Tamilselvan L, Sankaranarayanan V. Prevention of co-operative black hole attack in MANET. Journal of Networks. MAY 2008;**3**(5):15-20

[10] kurosawa S, Jamalipour A. Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. International Journal of Network Security. Nov 2007;**5**:338-346

[11] Aad I, Hubaux PJ, Knightly WE. Impact of denial-of-service attacks on ad-hoc networks. IEEE-ACM Transactions on Networking. 2008;**16**(4):791-802

[12] Mishra D, Jain KY, Agarwal S. "Behavior analysis of malicious node in the different routing algorithms in mobile ad hoc network (MANET)", Proceeding from ACT'09: IEEE advances in computing. Control and Telecommunication Technologies, Trivandrum. December 2009;**28-29**:621-623

[13] Buchegger S, Boudec JYL. A Robust Reputation System for Mobile Ad-hoc Networks. Technical Report, IC/2003/50, EPFL/IC/LCA. Lausanne, Switzerland. July 2003

[14] Deng H, Li W, Agrawal DP. Routing security in wireless Ad Hoc networks. Cincinnati University of Cincinnati, OH, USA; IEEE Communications Magazine. ISSN: 0163-6804, Vol.40, Oct. 2002. pp.70-75

[15] Lee S, Han B, Shin M. Robust Routing in Wireless Ad Hoc Networks. 2002 International Conference on Parallel Processing Workshops. Vancouver, Canada; Aug 2002. pp. 73-78 DOI: 10.1109/ICPPW.2002.1039714

[16] Kurosawa S, Nakayama H, Kat N, Jamalipour A, Nemoto Y. Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. International Journal of Network Security. Nov. 2007;**5**(3):338-346

[17] P.A.R Kumar, S.Selvakumar, "Distributed denial-of-service (DDoS) threat in collaborative environment - a survey on DDoS attack tools and Traceback mechanisms", IEEE International Advance Computing Conference (IACC 2009), pp. 1275-1280, March, 2009

[18] Dokurer S, Erten YM, Can EA. Performance analysis of ad-hoc networks under black hole attacks. Proceeding from SECON'07: IEEE Southeast Conference. Richmond, 22-25 March 2007, pp. 148-153

[19] Kim C, Talipov E, Ahn BA reverse AODV routing protocol in ad hoc mobile networks. The International Conference on Emerging Directions in Embedded and Ubiquitous Computing (EUC'06). Seoul, 1-4 August 2006, pp. 522-531. Springer, 2006

[20] Salem A, Hamamreh R. Efficient mechanism for mitigating multiple black hole attacks in MANETs. Journal of Theoretical and Applied Information Technology (JATIT). Jan 2016;**83**(1):156-164

[21] Hamamreh R, Jamoos M, Zagha R. DILH: Data integrity using linear combination for hash algorithm. ICITeS-Edas-1569740315-18

[22] The Network Simulator ns-2. [Online]. Available: http://www.isi.edu/nsnam/ns

[23] Hegde N, Manvi S. Simulation of wireless sensor network security model using NS2. International Journal of Latest Trends in Engineering and Technology (IJLTET). May 2014;**4**

[24] Manikandan C, Parameshwaran R, Hariharan K, Kalaimani N, Sridhar KP. Combined security and integrity agent integration into NS-2 for wired, wireless and sensor networks. Australian Journal of Basic and Applied Sciences. 2013;**7**(7):376-382. ISSN 1991-8178

IntechOpen