On Securing Atomic Operations in Multicast AODV

AHMED M. ABDEL MOAMEN1,* AND HAITHAM S. HAMZA1,*

1 University of Saskatchewan
E-mail: agents.usask.ca, ama883@mail.usask.ca
2 ANSR Laboratory, Faculty of Computers and Information, Cairo University
E-mail: hhamza@ansr.cu.edu.eg

Received: August 2, 2013. Accepted: January 1, 2014.

Multicast is an important communication pattern in Mobile Ad-hoc Network (MANET) that involves the transmission of packets to a group of two or more hosts, and thus can support group-oriented applications. Securing multicast routing in MANET is crucial in order to enable effective and efficient implementations of such applications. However, security techniques typically add more complexity to the protocol, and thus, may adversely impact its performance. Thus, a key objective in designing secure multicast routing protocols is to add security while reducing overhead. In this paper, we present a new approach, namely, the atomic security approach for securing the well-known Multicast Ad-hoc On-demand Distance Vector (MAODV). The underlying concept of the proposed approach is to secure basic (atomic) operations in the MAODV instead of the conventional approach of securing functional operations. Extensive simulation results show that the proposed approach based on securing atomic operations does not only decrease the byte overhead by 234% and improve Packet Delivery Ratio (PDR) by 16% as compared to conventional approaches, but it also provides a scalable framework to effectively and efficiently address future attacks on MAODV protocol.

Keywords: Mobile ad-hoc network (MANET), multicast routing protocol, security techniques, multicast routing attacks, MAODV.

1 INTRODUCTION

Multicast is an important communication pattern that involves the transmission of packets to a group of two or more hosts, and thus can support...
group-oriented applications. Securing multicast routing in mobile ad-hoc networks (MANETs) is crucial in order to enable effective and efficient implementations of such applications. However, security techniques typically add more complexity to the protocol, and that is may adversely impact its performance. Thus, a key objective in designing secure multicast routing protocols is to add security while reducing overhead [9].

Multicast Ad-hoc On-demand Distance Vector (MAODV) protocol [14, 15] is one of the well-known multicast routing protocol in MANETs. MAODV is susceptible to attacks by outsiders as well as malicious insiders. Some of these attacks are effectively confronted by security countermeasures, and others are not efficiently confronted, that is countermeasures increase overhead and reduce protocol performance.

Considerably conventional security techniques for MAODV [13] focus only on securing its functional operations (e.g., route discovery and link repair [15]). These functional operations are composite of several basic operations. In other words, it can be decomposed into smaller operations of which some are similar or identical. Thus, securing individual functional operations may unnessirly increase overhead and reduce protocol performance. Accordingly, we address this problem by proposing new security approach for securing basic operations, we call it the atomic security approach. The concept of securing atomic operations is to exploit the redundancy among the functional operations of the MOADV protocol. We believe that, by securing these atomic operations (which require small control overheads to guarantee the integrity and authentication) several multicast attacks can be confronted without a significant degradation in the network performance.

The objective of the proposed atomic security approach is two fold: (1) Reduce redundancy, to improve efficiency, and (2) Increase modularity, to efficiently secure the protocol against new attacks. For evaluating the second objective, we identify and describe, three new protocol-dependent attacks on multicast operations of MAODV namely, Group Leader Selection (GLS); False Link Breakage (FLB); Group Leader Pruning (GLP) attack. Then, we study the impact of proposed atomic security approach on the new identified attacks, simulation results show that the atomic security approach is effective and efficient under the newly identified attacks.

The contributions of this paper can be summarized as follows: (i) Propose a new atomic security approach and use it to develop a security framework to secure the MAODV protocol in a modular and efficient way; (ii) Define three new multicast attacks on MAODV and demonstrate how the proposed security framework can be used to efficiently confront the newly identified attacks.

The rest of the paper is organized as follows. Section 2 presents a relevant background work, including a brief overview on the main multicast
operations of MAODV protocol, short description for the known MAODV multicast attacks, and describes the new identified protocol-dependant attacks on multicast operations of MAODV. Securing atomic operations in MAODV are presented in Section 3. Section 4 presents the performance simulation study. Section 5 concludes the paper.

2 ATTACKS ON MAODV

Several attacks on routing protocols for MANETs have been described in the literature (e.g., [8, 10, 13]). Figure 1 shows the different types of attacks that target the unicast as well as the multicast operations of the MAODV protocol. Attacks on unicast operations of MAODV such as rushing [6], blackhole [10], neighbor [10], jellyfish [10], location disclosure [4], denial of service [2], wormhole [11] and routing table poisoning [16] are efficiently confronted in literature [11,16,17]. Therefore, in this paper, we do not investigate to secure MAODV against this type of attacks.

Multicast operation attacks on MAODV can be classified into two types:

1. **Inefficiently Confronted Attacks**: In which, some security solutions are proposed in literature [13] to find effective but inefficient countermeasures to this kind of attacks.
2. **New Attacks:** In this paper, we identify and describe, three new protocol-dependant attacks on multicast operations of MAODV protocol.

In this section, we look at relevant background work, including prior work on the MAODV multicast operations, some known attacks on MAODV’s multicast operations. In addition to describing the newly identified attacks on MAODV.

2.1 MAODV Overview

MAODV [14, 15] creates bi-directional shared multicast trees connecting multicast sources and receivers. These multicast trees are maintained as long as group members exist within the connected portion of the network. Each multicast group has a group leader whose responsibility is maintaining the group sequence number, which is used to ensure freshness of routing information [15].

Route Requests (RREQs), Route Replies (RREPs), Multicast Activations (MACTs), and Group Hellos (GRPHs) are the control message types utilized by MAODV. Each multicast group has a unique multicast group address. According to the MAODV specification in [14, 15], each multicast group is organized by using a tree structure, composed of the group members and several routers, which are not group member but must exist in the tree to connect the group members.

*Route discovery and link activation operation*

When a mobile node wishes to join a multicast group, it originates an RREQ message. Only group members of the desired multicast group may respond to the source of the RREQ. Each node receiving the request saves a route back to the source of the request, the RREP can be unicast back to the source from any node able to satisfy the request. After waiting for a specified period to receive RREPs, the requester node selects the best route to the multicast tree and unicasts a MACT message with ‘J’ (join) flag set, to the next hop which is on the selected route. This message officially grafts the selected route onto the existing multicast tree [15].

*Link breakage repair operation*

When a node discovers connectivity loss with the multicast tree neighbor, the downstream neighbor is responsible for correcting the link breakage. The downstream node sends a RREQ with its current hop count. Only multicast tree member nodes that have distance to the group leader equal or less than the one set in the hop count may answer with RREP. This prevents the nodes on the same side of the break as the initiator of the RREQ from answering and thus creating possible loops. If the repair leads to a situation, where the node’s new distance to the group leader is greater than the old one, then the
node must inform its downstream nodes about that new distance. This is done with MACT with ‘U’ (update) flag set [14].

Tree pruning operation
A multicast group member can revoke its member status at any time, if and only if it is a leaf node, it unicasts to its next hop on the tree a MACT message with ‘P’ (prune) flag set. It then deletes the multicast group information for that multicast group from its multicast route table. When its next hop receives this message, it deletes the sending node’s information from its list of next hops for the multicast tree.

If the removal of the sending node causes this node to become a leaf node, and if this node is also not a member of the multicast group, it may in turn prune itself by sending its own MACT message up the tree. If a non-leaf node wants to leave the multicast group, it sends MACT message to all its neighbors. When its downstream node(s) receive this message, it propagates RREQ message though the network and join to a new upstream node. Then the non-leaf node can revoke its member status and leave the multicast group [14].

Tree merging operation
Tree merge can be detected when a tree member with a smaller group leader address receives a GRPH generated by another group leader with a larger address for the same group. The tree member initiates the merge by unicastly sending a RREQ with ‘R’ (repair) flag set to the group leader in order to rebuild the tree. This RREQ propagates from downstream to upstream till the leader is reached. If the leader has not permitted other nodes to rebuild the tree, it can send back a RREP with ‘R’ flag set to that request node. When receiving the RREQ packet, the reverse route to the request node is formed, so the RREP packet follows this reverse route to the request node [15].

2.2 Inefficiently Confronted Attacks
In this sub-section, we describe some attacks on multicast operations of MAODV; in which, effective but inefficient countermeasures [13] are proposed that degrade the network performance. Table 1 summarizes the described multicast attacks on MAODV.

<table>
<thead>
<tr>
<th>Attack</th>
<th>Confronted operation</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>MACT(J)-MTF</td>
<td>Link activation using RREQ packet</td>
<td>Mesh topology</td>
</tr>
<tr>
<td>MACT(P)-PART</td>
<td>Tree pruning using MACT packet</td>
<td>Tree partitioning</td>
</tr>
<tr>
<td>RREP(J)-PART</td>
<td>Link repair using RREP</td>
<td>Tree splitting</td>
</tr>
</tbody>
</table>

TABLE 1
Attacks on Multicasting Operations in MAODV
Multicast Activation includes Join flag - Multicast Tree Formation (MACT(J)-MTF) attack

A malicious node can launch an attack against link activation operation by selecting multiple routes to the multicast group. It broadcasts a RREQ message with ‘J’ flag set to neighbor nodes in order to join the multicast group, it may receive multiple RREPs in response to its RREQ from neighbor nodes.

The malicious node doesn’t select the best route and send MACT message with ‘J’ flag set to the selected reverse route; but instead of that, it sends a MACT message to all received RREPs, which will result in many extra edges being grafted on to the multicast tree, in other words, it will create mesh topology instead of tree topology. Besides, it will result in unnecessary packet duplication and energy expenditure. It is clear that, a single malicious node can increase the energy expenditure of many other nodes by sending extra packets, so this attack is considered a resource consumer attack [13].

Figure 2 illustrates the three steps of this attack. Figure 2(a) shows the malicious node (M) broadcasting a RREQ request. Figure 2(b) shows the
route replies sent to node (M). 2(c) shows how malicious node (M) connected to the multicast tree, M sends MACT packets to all the nodes (A, B and C) from which it received RREPs, and many unnecessary branches being grafted on the multicast tree.

**Multicast Activation includes Prune flag - Multicast Tree Partition (MACT(P)-PART) attack**

A malicious node can launch attack against tree pruning operation by pruning group member(s) from the multicast tree, first it impersonates a tree node, and sends a prune control message MACT with ‘P’ flag set to its downstream nodes in the multicast tree. If a downstream node is a non-member and has only one downstream link, it also prunes itself and sends a similar prune message to its downstream node. This may lead to the multicast tree being partitioned [13].

Figure 3 illustrates the two steps of this attack. Figure 3(a) shows that malicious (M) impersonates (A) and sends a MACT packet with ‘P’ flag set to A’s immediate downstream node (B). Figure 3(b) shows that node (B) prunes itself from the tree and forwards the MACT with ‘P’ flag to its downstream node and its downstream node C forwards the MACT to its downstream node and so on, until node (E) becomes another group leader.

**FIGURE 3**
An Example of MACT(P)-PART Attack
Route Reply includes Join flag - Multicast Tree Partition (RREP(J)-PART) attack

A malicious node can launch attack against link repair operation by partitioning the multicast tree into two or more partitions. When a node’s link to its neighbor node in the multicast tree breaks, the downstream node attempts to repair the link by broadcasting a RREQ packet with ‘J’ flag set. Only tree members with current group sequence number greater or equal to the sequence number indicated in the RREQ packet and whose hop count from the group leader indicated in the RREQ packet should respond with a RREP to this request.

A malicious node may respond with a RREP message with sequence number higher than the current group sequence number and with a false hop count that is smaller than the actual one. This results in the sender node accepting the malicious node as its upstream node. Thus all malicious’s downstream nodes get partitioned from other group members by the malicious node [13].

Figure 4 illustrates the two steps of this attack. Figure 4(a) shows that the link between (A) and (B) breaks. (B) starts route discovery by broadcasting RREQ packets with ‘J’ flag set and the group sequence number and its hop count from the group leader which is three. Malicious node (M) respond with a RREP message with sequence number higher than the current group sequence number, and with a false hop count. This results in (B) accepting the malicious node as its upstream node, partitioning its downstream nodes from other group members.
2.3 Newly Identified Multicast Attacks on MAODV

In this sub-section, we identify and describe, three new protocol-dependant attacks on multicast operations of MAODV namely, Group Leader Selection (GLS), False Link Breakage (FLB), and Group Leader Pruning (GLP) attack [3]. For each attack, we implement a scenario to show its impact on the network performance. Table 2 summarizes the described multicast attacks.

**Group Leader Selection (GLS) attack**

A malicious node can launch attack against group leader selection operation by deceiving non-group members as well as, group members to become a group leader even if it is outside the multicast tree. In normal MAODV operations, If a node sends a RREQ to join a multicast group ‘J’ flag set and after RREQ retries attempts does not receives a response, it then becomes the multicast group leader [14, 15].

The malicious node exploits this feature to announce itself as a new group leader and initializes the multicast group sequence number and then broadcasts a GRPH message (with hop count less than the existing group leader) to inform network nodes that it is now the group leader for the multicast group. Then it launches group leader miss-functionality attacks, such as: not continually maintains the multicast tree, sending GRHP messages with old sequence numbers, and not performing partition merge operation steps.

Figure 5 illustrates the two steps of GLS attack. Figure 5(a) shows that nodes (A, C and D) want to join the multicast tree leaded by group leader (L). Malicious node (M) deceives these nodes to take it as their group leader by broadcasting a GRPH message to them with hop count less than node (L). That will result constructing a new multicast tree leaded by node (M) (Figure 5(b)).
False link breakage (FLB) attack
A malicious node can launch this attack against the multicast tree by initiating a link repair operation for unreal link breakage in the multicast tree. First, the malicious node must join the multicast tree by broadcasting a RREQ with ‘J’ set to join the multicast group [14, 15], and then it reports about false link breakage between it and its upstream node. The malicious node broadcasts a RREQ with with ‘J’ flag set with a group leader hop count greater than the real hop count. That will leads to nodes on the same side of the break as the malicious node may answer this RREQ and thus creating possible loops in the multicast tree.

Figure 6 illustrates the two steps of FLB attack. Figure 6(a) shows that malicious node (M) reports about virtual link breakage between it and node (B). Node (M) sends RREQ with ‘J’ flag set message to nodes (A and C) with hop count greater than two (the real hop count from group leader), nodes (A and C) believes that node (M) is a downstream node, therefore they replies with RREP message and new edges MC and MA are created causing loop in the multicast tree (Figure 6(b)).

Group leader pruning (GLP) attack
A malicious node can launch this attack against the multicast tree by pruning the group leader from the multicast tree. It must first impersonate the group leader, and then it broadcasts a MACT message with ‘P’ flag set to all group leader’s downstream nodes. In normal MAODV operations in [14], when a downstream node receives a MACT message with ‘P’ flag set from upstream node, it propagates RREQ message though the network and join to
a new upstream node. In other words, the group leader is forced to revoke the multicast tree. That may result that the multicast tree may be partitioned into multiple trees and consequently the network performance will be degraded.

Figure 7 illustrates the two steps of GLP attack. Figure 7(a) shows that malicious node (M) listens to control packets outgoing from group leader

![Figure 6](image6.png)

**FIGURE 6**
False link breakage attack

![Figure 7](image7.png)

**FIGURE 7**
Group leader pruning attack
(L) to his downstream nodes in order to know its IP address and group ID. Node (M) uses this information to impersonate the group leader (L) and sends MACT message with ‘P’ flag set to nodes (A and B) to indicate that node (L) wants to prune itself and leave the multicast group. Figure 7(b) shows that the multicast group is now partitioned into two groups led by nodes (A and B) that will cause the network performance be degraded.

3 MAODV SECURITY APPROACH BASED ON ATOMIC OPERATIONS

In this section, we present the concept of the proposed atomic security approach, and its three security modules. In addition, the impact of the proposed atomic approach on known and newly identified multicast attacks.

3.1 The Concept of the Proposed Atomic Security

Conventional security techniques for MAODV focus only on securing functional operations (e.g., route discovery and link repair) [13]. Functional operations; however, do share several basic (atomic) operations. Thus, securing individual functional operations may increase overhead and reduce protocol performance. Accordingly, we propose the concept of securing atomic operations to exploit the redundancy among the functional operations of the MOADV protocol. To demonstrate the concept of the atomic operations, we explain how the functional operations of the MAODV can be decomposed into smaller overlapped operations.

Figure 8 shows the decomposition of the various MAODV operations into layers. As shown in the figure, the top layer contains conventional functional operations...
operations of the protocol: Route discovery, link breakage repair, tree pruning, and tree merging operation. These operations are not atomic as they can be decomposed into smaller operations, sum of which are shared among the various operations. For instance, the atomic operation send/receive RREQ is used in all the four functional operations. Thus, it can be identified as an atomic operation.

Following the same logic, Figure 8 shows the atomic operation layer that contains all the atomic operations in the MAODV protocol. In order to simplify the presentation, atomic operations can be grouped into categories as shown in the middle layer named Atomic Operation Categories given in Figure 8. Figure 9 shows another representation for the classification of the three layers to highlight the common atomic operations shared among the various MAODV functional operations.

By identifying the notion of the atomic operations, it is possible to rethink the way we use the secure routing protocols. In particular, securing related atomic operations can: (1) Reduce redundancy (and hence, improve efficiency) (2) Increase modularity, by reducing the complexity of securing the protocol against newly identified attacks. In this paper, we will demonstrate how these two benefits are realized by adopting the proposed atomic security approach.

Figure 10 presents the structure of the security framework built using the proposed atomic approach to secure the MAODV protocol.
3.2 Control Messages Authentication Module

*LHAP* [18] was specifically designed for MANETs; it introduces the idea of hop-by-hop authentication that uses two hash keys at every node. LHAP does not require loose time synchronization. It is also very efficient and it authenticates packets instantly, reducing latency and eliminating the need for a cache at every node. LHAP uses two hash keys at every node in the network since LHAP is lightweight, efficient hop-by-hop authentication scheme, and does not require loose time synchronization, we use it to authenticate the control packets (RREQ, RREP, GRPH, MACT), in which the MAODV’s functional operations (described in Sub-section 2.1) uses to perform its routing operations. Each node in network has a public key certificate signed by a trusted certificate authority (CA) and also an authentic public key of the CA is used.

Any control packets from unauthorized nodes are dropped, thus preventing them from propagating through the network. A packet that needs multiple hops before reaching its destination, thus gets authenticated by each node on its path. For example, in the route discovery operation: when a mobile node wants to join the multicast group, it broadcasts an RREQ message to all its neighbors. This RREQ message is authenticated in every hop it travels, until it reaches to a group member that can reply on it. If this RREQ is originated from unauthorized node, this RREQ will be dropped from all intermediate nodes, that will result this can’t join the multicast group and can’t launch attacks against the network.

3.3 Group Certificate Module

*TESLA* [12] is a very efficient multicast stream authentication protocol. It uses symmetric cryptographic function that uses public one-way hash chain key. Packets are not authenticated at every hop, instead they are only authenticated by the final receiver after a delay of several seconds, i.e., end-to-end authentication. The packets are held in a cache at the receiving node until the hash key used to authenticate them has been disclosed by the sender. If the hash key can regenerate the MAC of the packet, the packet is considered
authentic; otherwise, it is dropped. Intermediate nodes simply forward the packets without authentication. In addition, TESLA requires the clocks of all the nodes in the network to be loosely synchronized.

TESLA is used in creating the group membership certificate, which supports source authentication in MAODV. Every group member must be signed by the Certification Authority (CA), this type of certificates called group certificate which considered the key identity for the group member to join the multicast group. This certificate contains the group ID, group private key, and the group public key used for signing the certificate. When a group member sends a control message (i.e., RREQ, RREP, MACT, or GRPH), it appends its own certificate to the control packet. Every legitimate group member can verify the correctness of this certificate using group, group private, and public keys. If an intermediate group member fails to verify the control message, it will drop it.

3.4 Hop Count Authentication Module
Hash chains [5] can be used in MAODV to authenticate the hop count of nodes from the group leader. Every time a node wants to send a control message, it generates a random number called seed number. The hash field in the signature extension in the control packets is set to that seed number. The function used to compute the hash key is set in the hash function field. Since this field is signed, a forwarding node will only be able to use the same hash function that the originator of the routing message has selected. If a node cannot verify or forward a routing message because it does not support the hash function that has been used, then the node drops the packet.

3.5 Impact of Atomic Approach on Multicast Attacks
We discuss below the impact of atomic security on multicast attacks, and how each attack is prevented or mitigated:

\textit{MACT(J)-MTF attack}

MACT(J)-MTF is prevented by control messages authentication module. In this attack, the malicious node broadcasts a RREQ message neighbor nodes in order to join the multicast group, then it proceed its attack against the protocol. This RREQ message is authenticated with LHAP scheme using a public key certificate signed by a trusted CA in every node it propagates. That will cause that the RREQ packet will be dropped and this attack is properly prevented.

\textit{MACT(P)-PART attack}

MACT(P)-PART is prevented by group certificate module. In this attack, at first the malicious node must impersonate a tree node, in order to launch its
attack against the tree pruning operation. The malicious node can’t include a legitimate group membership certificate in its control messages, so it can’t impersonate a tree node, that will result this attack is properly prevented.

**RREP(J)-PART attack**
RREP(J)-PART is prevented by hop count authentication module. In this attack, the malicious node sends a RREP message with a false hop count that is smaller than the actual one, in order to make the RREQ’s sender node accepts the malicious node as its upstream node. Using our hop count authentication module, the sender node will drop this RREP, and thus attack is prevented.

**Group leader selection attack**
In GLS attack, the malicious node broadcasts a GRPH message to all nodes in order to announce itself as a new group leader. When a legitimate node receive this message, it will discover that the message’s sender is unauthorized node (by control messages authentication), so it will drop all messages initiated from that malicious node, and this attack is prevented.

**False link breakage attack**
In FLB attack, the malicious node must join the multicast tree by broadcasting a RREQ with J set. Intermediate group members will drop this message as it is not signed by a trusted CA in the network, and this attack is prevented.

**Group leader pruning attack**
In GLP attack, the malicious node impersonate the group leader and broadcasts a MACT message with P flag set to all group leaders downstream nodes in order to prune the group leader from the multicast tree. The malicious node can’t include a legitimate group membership certificate in its MACT message, so it can’t impersonate a tree node (by group certificate), that results this attack is prevented.

### 4 PERFORMANCE EVALUATION

This section presents the study used to evaluate the proposed approach via simulation. The section shows results obtained to evaluate efficiency and modularity of the proposed atomic approach.

#### 4.1 Simulation Setup and Evaluation Methodology

The network simulator QualNet [1] is used to evaluate the performance of the network that shows the impact of the attacks and the proposed atomic
approach on it. We modified the MAODV source code to develop the attacker behavior that run on malicious nodes in the simulation environment. Table 3 summarizes the simulation parameters used in simulation while Table 4 lists the default MAODV parameters.

The simulated scenario consists of a network with thirty nodes and one multicast group with ten only members. All the group members join the multicast group at the beginning of the simulation leading to the construction of the multicast tree. There is extra node acts as base station, which is responsible for the distribution of certificates, this base station plays the role of the central LHAP and TESLA certificate authority. The group certificates in our simulation use a 512 bit public key and 16-byte signature as in Ariadne [7]. Each simulation was run for 180 seconds. For each set of experiments, ten runs were performed. The average values are used in plotting the graphs.

Packet Delivery Ratio (PDR) is used as a performance metric to analysis the impact of the multicast attacks on the network performance, as well as evaluating the proposed approach after applying it on the performance of simulations.
MAODV. The total packets transmitted is used as a metric to evaluate the network performance under the multicast tree extra edges attack, as this attack targets to graft extra edges to the multicast tree, that result sending additional packets that resume the network resources.

For each attack, we run four different scenarios, in addition to making comparison between our secured MAODV using atomic approach and the secured MAODV using functional approach proposed by Roy in [13], in order to show the impact of the attack and the effect of the proposed security framework, as the following:

- **No security and no attackers**: We run the simulation 10 times in normal operation without any attacker in the environment. We record the PDR of all nodes in the multicast group.
- **No security and two attackers**: We implement the attacker malicious behavior and run it on 2 nodes in the simulation environment, and then we run the experiments and take its average values in order to capture accurate PDR values.
- **Atomic security and two attackers**: We implement our security framework on all nodes in the network in presence of the 2 attackers, then we run the experiments and record the PDR values in this case.
- **Functional security and two attackers**: The comparative security framework proposed by Roy in [13] in the presence of 2 attackers.

### 4.2 Evaluation of Redundancy Reduction

Figure 11 depicts the simulation scenarios for attacks described in Subsection 2.2 for various speeds of mobile nodes, as the following:

1. **MACT(P)-PART attack**: [Figure 11(a)] this attack degrades the PDR with 22% compared to unsecured MAODV. Using the functional security approach, the PDR is degraded by 7%, whereas using our atomic security approach, the PDR is degraded by only 3%, that shows an improvement of 18%.
2. **RREP(J)-PART attack**: [Figure 11(b)] this attack degrades the PDR with 24% compared to unsecured MAODV. Using the functional security approach, the PDR is degraded by 6%, whereas using our atomic security approach, the PDR is degraded by only 2.5%, that shows an improvement of 14%.
3. **MACT(J)-MTF attack**: [Figure 11(c)] this attack increases the number of bytes transmitted by 60% compared to unsecured MAODV. Using the functional security approach, the number of bytes transmitted increases by 16%, whereas using our atomic security approach, the number of
bytes transmitted increases by only 4%, that shows an improvement of 20%.

Figure 11(d) gives the byte overheads caused by the additional control overheads which added by the proposed countermeasures, due to control packet authentication and the increased control packet sizes. Compare to unsecured MAODV’s byte overheads, the functional security approach increases the byte overheads by 300%. Whereas our atomic security approach increases the byte overheads by 66% only, that shows an improvement of 234%.

We study the performance of the atomic security framework with varying some simulation parameters and showing the effect of these parameters in performance and overheads. The number of nodes in the multicast group is
increased to fifteen node instead of ten, as well as increasing the number of attackers to four and six instead of two.

- Figure 12(a) shows that MACT(P)-PART attack with presence of 4 and 6 attackers degrades the PDR with 29% and 40%, respectively. Whereas using our atomic framework in presence of 4 and 6 attackers, the PDR is degraded by only 6% and 9%, respectively. That shows an improvement of 79% and 77%, respectively.
- Figure 12(b) shows that RREP(J)-PART attack with presence of 4 and 6 attackers degrades the PDR 34% and 48%, respectively. Whereas using our atomic framework in presence of 4 and 6 attackers, the PDR is degraded by only 6% and 11%, respectively. That shows an improvement of 82% and 77%, respectively.
• Figure 12(c) shows that MACT(J)-MTF attack increases the number of bytes transmitted with presence of 4 and 6 attackers by 75% and 120%, respectively. Whereas using our atomic framework in presence of 4 and 6 attackers, the number of bytes transmitted increases by only 10% and 19%. That shows an improvement of 65% and 101%, respectively.

4.3 Evaluation of Modularity
Figure 13 depicts the simulation scenarios for the newly identified attacks described in Sub-section 2.3 for various speeds of mobile nodes, as shown in the figure, we conclude the following regarding the PDR:

(1) **Group leader selection attack:** [Figure 13(a)] GLS attack degrades the PDR with 34% compared to unsecured MAODV. Whereas using our
proposed countermeasures, the PDR is degraded by only 4%, that shows an improvement of 88%.

(2) **False link breakage attack**: [Figure 13(b)] FLB attack degrades the PDR with 35% compared to unsecured MAODV. Whereas using our proposed countermeasures, the PDR is degraded by only 6%, that shows an improvement of 83%.

(3) **Group leader pruning attack**: [Figure 13(c)] GLP attack degrades the PDR with 28% compared to unsecured MAODV. Whereas using our proposed countermeasures, the PDR is degraded by only 4%, that shows an improvement of 85%.

5 CONCLUSION

Functional security techniques for MAODV may lead to low performance and high overheads due to security overhead redundancy. This paper addresses this problem and proposes an approach for securing atomic operations instead of functional operations. We show, via simulation, that the proposed approach can reduce redundancy and improve modularity. Moreover, we identify and describe, three new protocol-dependant attacks on multicast operations of MAODV. We study the impact of proposed atomic security approach on the newly identified attacks. Extensive simulation results confirm that the atomic approach can improve performance and decrease overheads under attack compared to functional security approach.

REFERENCES


