New Attacks and Efficient Countermeasures for Multicast AODV

Ahmed. M. Abdel Mo’men, Haitham. S. Hamza, IEEE Member, and Iman. A. Saroit

Abstract—Security in multicast routing in MANETs is crucial in order to enable effective and efficient multicast-based applications. Multicast Ad-hoc On-demand Distance Vector (MAODV) protocol is one of the well-known multicast routing protocol in MANET. In this paper, we identify and describe, for the first time, 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. For each attack, we implement a scenario to demonstrate the impact of the attack on the performance of the network. Implemented scenarios show a considerable degradation in the Packet Delivery Ratio (PDR) of the protocol. Accordingly, we propose security countermeasures for the identified attacks. Simulation results of the secured and unsecured MAODV show that the proposed countermeasures are effective and efficient.

Index Terms—Mobile ad-hoc network (MANET), multicast routing protocol (MRP), mobile node (MN), security techniques, multicast routing attacks, MAODV.

I. INTRODUCTION

As MANETs continue to grow in capability and are becoming increasingly useful in many emerging applications, security is becoming inevitably a pressing property in the design of such networks. Multicast Ad-hoc On-demand Distance Vector (MAODV) protocol [1], [2] is one of the well-known multicast routing protocol in MANETs. MAODV is susceptible to attacks by outsiders as well as malicious insiders. Attacks on MAODV can be divided into two broad categories, unicast attacks and multicast attacks.

In this paper, we focus on multicast attacks that confront the MAODV’s functional multicast operations shown in Figure 1. We further classify multicast attacks to two types: (1) Confronted attacks. In which, some security solutions are proposed in literature to find effective countermeasures to this kind of attacks. In this paper, we identify and describe, for the first time, 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. We call this type (2) Non-confronted attacks in which, no dedicated security solutions are proposed to them yet. For each attack, we implement a scenario to show its impact on the network performance.

The objective of this paper is to provide security countermeasures for the identified multicast attack to guarantee the integrity and authentication in the multicast routing operations of the MAODV protocol. The contribution of this paper is two fold:

1) Identify and describe three new multicast attacks on MAODV. For each attack, we implement a scenario to show its impact on the network performance, as well as showing via simulation, that the performance of MAODV under attack is heavily degraded.

2) Propose security countermeasures for securing MAODV against the identified attacks in order to guarantee the integrity and authentication without degradation in the performance of the protocol.

The rest of the paper is organized as follows. Section II presents a relevant related work. Section III presents brief overview on the main multicast operations of MAODV. Section IV presents short description for the main types of attacks on MAODV operations. The proposed security countermeasures are presented in Section V. Section VI contains the performance simulation study that shows that our countermeasures are effective and efficient. Section VII concludes the paper.

II. RELATED WORK

Many attacks on routing protocols for MANETs have been described in the literature [3], [4], [5]. Several unicast attacks on MAODV are presented in literature such as; rushing [6], blackhole [7], neighbor [7], jellyfish [7], location disclosure [8], denial of service [9], wormhole [10], and routing table poisoning [11] attack. All these attacks are efficiently confronted in [12], [11], [10], [13], [14]. Therefore in this paper, we not investigate to secure MAODV against these attacks.

Several approaches presented in literature aim to enhance the security of multicast routing in MANETs such as SORB [15], BSMR [16], DIPLOMA [17], and SRMAODV [18]. All these approaches address security aspects related to cover attacks that confront the unicast operations of its extended protocols. On the other way, some attacks described in [3] targets the multicast operations of MAODV. The authors also propose an authentication framework to protect MAODV against the identified attacks.

III. MAODV MULTICAST OPERATIONS

MAODV [1], [2] is a multicast routing protocol for ad hoc networks that dynamically constructs a shared multicast tree.
which connects the group members possibly via some non-member nodes [2]. It offers quick adaptation to dynamic link conditions, low processing, low memory overhead, and low network utilization. It 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 [1].

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 [1], [2], 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. We say the group members and the routers are all tree members and belong to the group tree.

Each node in the network maintains three tables [2]: (1) Unicast route table, it records the next hop for routes to other destinations for unicast traffic; (2) Multicast route table, it lists the next hops for the tree structure of each multicast group. Each entry represents one group tree structure; (3) Group leader table, it records the currently-known multicast group address with its group leader address and the next hop towards that group leader when a node receives a periodic GRPH message.

For each multicast tree in the network, the group member that first constructs the tree is the group leader for that tree, and it is responsible for maintaining the group tree by periodically broadcasting GRPH messages in the whole network, in which maintains the sequence number for the multicast group and increased periodically by the group leader [2].

The multicast operations described in this section are route discovery, link breakage repair, tree pruning, tree merging and group leader selection.

A. Route discovery and link activation

MAODV discovers multicast routes on demand using a broadcast route discovery mechanism employing RREQ and RREP messages [1]. When a mobile node wishes to join a multicast group, or has data to send to a multicast group but does not have a route to that 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 unicasted back to the source from any node able to satisfy the request.

In case of join requests, 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. If the RREQ is not a join request, any node with a fresh enough route (based on group sequence number) to the multicast group may respond. If an intermediate node receives a join RREQ for a multicast group of which it is not a member, or it receives a RREQ and does not have a route to that group, it rebroadcasts the RREQ to its neighbors [2].

B. Link breakage repair

The rapid changes in the network topology may lead to link breakage between two nodes. When a node discovers connectivity loss with the multicast tree neighbor, if it is the downstream neighbor, it is responsible for correcting the situation. Now, the node sends a RREQ with a multicast group leader hop count. This count contains the old distance of the node to the group leader. 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 [1].

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 message where the update ‘U’ flag is set. This MACT message is multicasted to all of the tree members, even upstream nodes. But upstream nodes see that this message comes from a downstream node and therefore discards the message.

C. Tree pruning

A multicast group member can revoke its member status at any time, if and only if, it is a leaf node [1]. It unicasts a MACT message with the ‘P’ flag set to its next hop on the tree. 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-leave node wants to leave the multicast group, it sends MACT message with the ‘P’ flag set 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-leave node can revoke its member status and leave the multicast group [2].

D. Tree merging

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 [2]. The tree member initiates the merge by unicastly sending a RREQ with a repair ‘R’ 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 to that request node. When receiving RREQ with 'R' flag, the reverse route to the request node is formed, so the RREP with 'R' flag follows this reverse route to the request node [1].

E. Group leader selection

A new group leader must be selected for the partitioned tree or when the group leader revokes its group membership [2]. When tree partition happens, and the current node is a group member, it will become the new group leader. Otherwise, it will force one of its tree neighbors to be the leader.

If the current node only has one downstream node, it cancels the entry for that group in its multicast route table, indicating it is no longer belongs to the tree, and sends out a MACT with 'P' flag set to this downstream node, indicating that it will leave the tree and the tree needs a leader. If the current node has more than one downstream node, it selects one downstream, change its direction from downstream to upstream, and sends a MACT with group leader ‘GL’ flag towards that node, indicating that it has other branch(es) in the tree and the tree needs a leader [1].

The downstream node can receive either a MACT with 'P' flag or a MACT with 'GL' from its upstream node. When receiving MACT with 'P' flag from its upstream, the node removes its upstream link from its Multicast Route Table. When receiving MACT with 'GL' flag from upstream, the node changes the upstream direction into downstream. Then if the node is a group member, it will be the new group leader. Otherwise, it continues the above procedure till a group member is reached and becomes the new group leader [2].

IV. NEW ATTACKS ON MAODV

We divided attacks on MAODV into two broad categories: (1) Unicast attacks, in which the attacks aren’t focused on the multicasting operations of the protocol, by another way, it attacks the unicast version of the protocol AODV [19] and when MAODV extends AODV, it extends also the related attacks on it; (2) Multicast attacks, in which attacks are focused on the multicast operations of the protocol, as this type of attacks confront MAODV’s multicast operations. Figure 2 shows the different types of attacks that target the unicast as well as the multicast operations of the MAODV protocol.

Some attacks described in [3] targets the multicast operations of MAODV. We classify these attacks into two categories: (1) Confronted attacks. In which, some security solutions are proposed in [3] in order to find effective countermeasures to this kind of attacks. In this paper, we identify and describe, for the first time, three new protocol-dependant attacks on multicast operations of MAODV namely, Group Leader Selection (GLS); False Link Breakage (FLB); Group Leader Pruning (GLP) attack. We call this type (2) Non-confronted attacks in which, no dedicated security solutions are proposed to them yet.

For each attack, we describe the attacker’s malicious behavior in confronting the multicast operations of MAODV, as well as providing simple scenario of the attack illustrated with descriptive figures for clarifying the attacker malicious steps. Table I summarizes the multicast attacks on MAODV described in this section.

A. 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 [1]. 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.

TABLE I

<table>
<thead>
<tr>
<th>Attack</th>
<th>Source</th>
<th>Confronted operation</th>
<th>Attack outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group leader selection</td>
<td>External</td>
<td>Group leader selection using GRPH</td>
<td>GL miss functionality tasks</td>
</tr>
<tr>
<td>False link breakage</td>
<td>Internal</td>
<td>Link repair using RREQ (J)</td>
<td>Loop in multicast tree branch(s)</td>
</tr>
<tr>
<td>Group leader pruning</td>
<td>External</td>
<td>Tree pruning using MACT (P)</td>
<td>Tree partitioning</td>
</tr>
</tbody>
</table>
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 3 illustrates the two steps of GLS attack. Figure 3(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 3(b)).

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’ flag set to join the multicast group [2], and then it reports about false link breakage between it and its upstream node. The malicious node broadcasts a RREQ 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 4 illustrates the two steps of FLB attack. Figure 4(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 4(b)).

C. 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 [2], 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 5 illustrates the two steps of GLP attack. Figure 5(a) shows that malicious node (M) listens to control packets outgoing from group leader (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 5(b) shows that the multicast group is now partitioned into two groups leaded by nodes (A and B) that will cause the network performance be degraded.

V. PROPOSED COUNTERMEASURES

In this section, we present the proposed countermeasures for securing MAODV against the identified attacks described in Section IV. The countermeasures described in this section are control messages authentication and group certificate.

A. Control messages authentication

LHAP [20] was specifically designed for MANETs and 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 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 [20], we use it to authenticate the control packets (RREQ,
RREP, GRPH, MACT), in which the MAODV’s functional operations (described in Section III) 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.

B. Group certificate

TESLA [21] 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 the MAODV. Every group member must be signed by the certification authority, 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 ID, group private and public keys. If an intermediate group member fails to verify the control message, it will drop it.

C. Impact of proposed countermeasures on attacks

All attacks discussed in Section IV are prevented by the proposed countermeasures. We discuss below how each attack is prevented or mitigated:

• **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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of nodes</td>
<td>30</td>
</tr>
<tr>
<td>Number of multicast group members</td>
<td>10</td>
</tr>
<tr>
<td>Pause time</td>
<td>40 sec</td>
</tr>
<tr>
<td>Simulation grid size</td>
<td>500m X 500m</td>
</tr>
<tr>
<td>Radio transmission range</td>
<td>200m</td>
</tr>
<tr>
<td>Traffic source</td>
<td>CBR at 2 packets/second</td>
</tr>
<tr>
<td>Mac protocol</td>
<td>802.15.4</td>
</tr>
<tr>
<td>Mac propagation delay</td>
<td>1 micro sec</td>
</tr>
<tr>
<td>Radio transmission power</td>
<td>3 dBm</td>
</tr>
<tr>
<td>Physical layer bandwidth</td>
<td>2 Mbps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active route timeout interval</td>
<td>3 secs</td>
</tr>
<tr>
<td>Route timeout interval</td>
<td>6 secs</td>
</tr>
<tr>
<td>Number of allowed hello loss</td>
<td>3</td>
</tr>
<tr>
<td>Hello interval</td>
<td>1 sec</td>
</tr>
<tr>
<td>Group hello interval</td>
<td>5 secs</td>
</tr>
<tr>
<td>Maximum allowed hello loss</td>
<td>2</td>
</tr>
<tr>
<td>Maximum RREQ retries</td>
<td>2</td>
</tr>
<tr>
<td>Time-To-Live (TTL) threshold</td>
<td>7</td>
</tr>
</tbody>
</table>
VI. PERFORMANCE ANALYSIS

The network simulator QualNet [22] is used in evaluating the performance of the network that shows the impact of the attacks discussed in Section IV and countermeasures described in Section V. We modified the MAODV source code to develop the attacker behavior that run on malicious nodes in the simulation environment. Table II summarizes the simulation parameters used in simulation and Table III lists the default MAODV parameters.

A. Simulation Setup

The simulated scenario consists of a network with thirty nodes and one multicast group with ten members only. All the group members join the multicast group at the beginning of the simulation leading to the construction of the multicast tree. There is a 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 [23]. Each simulation was run for 180 seconds. For each set of experiments, 10 runs were performed. The average values are used in plotting the graphs.

Packet Delivery Ratio (PDR) is defined as the ratio of the total number of data packets received by the multicast group members to the product of the number of data packets sent and the number of group members. We used PDR as a metric to analysis the impact of each attack defined in Section IV on the network performance, as well as evaluating the proposed countermeasures after applying it on the performance of MAODV. For each attack, we run three different scenarios to show the impact of the attack and the effect of our security countermeasures, as the following:

- MAODV with no security and no attackers: we run the simulation ten times in normal operation without any attacker in the environment, and record the PDR of all nodes in the multicast group.
- MAODV with no security and two attackers: we implement the attacker malicious behavior and run it on two nodes in the simulation environment, and then we run the experiments ten times and take its average values in order to capture accurate PDR values.
- Secured MAODV and two attackers: we implement our security countermeasures on all nodes in the network in presence of the two attackers, then we run the experiments and record the PDR values in this case.

B. Performance Study

Figure 6 depicts the simulation scenarios for the identified attacks for various speeds of mobile nodes, as shown in the figure, we conclude the following regarding the PDR:

1) Group leader selection attack: Figure 6(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 6(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 6(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%.

Figure 7 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, our countermeasures with presence of two attackers, increases the byte overheads by ratio up to 30%. This is considered an acceptable performance cost, given that the attacks prevented have a much larger impact on the performance of the protocol.

**VII. Conclusion and Future Work**

In this paper, we survey different types of attacks that confront the MAODV’s multicast operations. We identify and describe, for the first time, three new protocol-dependant attacks on multicast operations of MAODV namely, Group Leader Selection (GLS); False Link Breakage (FLB); Group Leader Pruning (GLP) attack. For each attack, we implement a scenario to show its impact on the network performance. We demonstrate by simulation that the performance MAODV under attack is heavily degraded to a large extent.

Accordingly, we propose security countermeasures for securing MAODV from the identified attacks. Simulation results show that our countermeasures are effective and efficient under attack. In particular, compared to unsecured MAODV, the proposed countermeasures improve the PDR with 85%. The additional control overhead added by proposed countermeasures increases the byte overheads by ratio up to 30%.

As a part of our future work, we plan to further evaluate the scalability and complexity of the proposed countermeasures. We can explore the impact the identified attacks in case of varying some simulation parameters such as increasing number of nodes in the multicast group and increasing number of attackers in order to show the effect of these parameters in performance and overheads of MAODV.

**References**


