Secure Multicast Routing Protocols in MANETs

Ahmed Abdel Moamen, Haitham S. Hamza, and Iman A. Saroit

The authors are with the Department of Information Technology, Cairo University, Giza, Egypt 12613

SUMMARY

A Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes that communicate with each other by forming a multi-hop radio network. Routing protocols in MANETs define how routes between source and destination nodes are established and maintained. Multicast routing provides a bandwidth-efficient means for supporting group-oriented applications. The increasing demand for such applications coupled with the inherent characteristics of MANETs (e.g., lack of infrastructure and node mobility) have made secure multicast routing crucial yet challenging issue. Recently, several multicast routing protocols have been proposed in MANETs. Depending on whether security is built-in or added, multicast routing protocols can be classified into two types: secure and security-enhanced routing protocols, respectively. This paper presents a survey on secure and security-enhanced multicast routing protocols along with their security techniques and the types of attacks they can confront. A detailed comparison for the capability of the various routing protocols against some known attacks is also presented and analyzed.

Copyright © 2011 John Wiley & Sons, Ltd.

KEY WORDS: Mobile ad-hoc network (MANET), multicast routing protocols (MRP), mobile node (MN), security techniques, multicast routing attacks, survey.

1. INTRODUCTION

A mobile ad-hoc Network (MANET) is a self-organized network of mobile nodes that communicate through wireless links. Self-creation, self-configuration, and self-administration are the most important features of this network [1, 2, 3, 4]. In MANETs, each node can act as both host and router (Figure 1). Two nodes can communicate directly if they are within the communication range of each other; otherwise, multi-hop communication is used.

Multicast is an important communication pattern that involves the transmission of packets to a group of two or more hosts, and thus is intended for group-oriented computing [3, 5, 6]. The use of multicasting in MANETs has many benefits. In particular, it can reduce the cost of communication and improve the efficiency of the wireless channel, when sending multiple copies of the same data by exploiting the inherent broadcasting properties of wireless transmission. Instead of sending data
Figure 1. Simple form of a mobile ad hoc network

via several unicast connections, multicasting minimizes channel capacity consumption, minimizes sender and router processing and energy consumption, and communication delay [7, 5].

In the field of multicast routing protocols and its security aspects, some research on the taxonomy of multicast routing protocols over MANETs have been carried out. Osamah et al. [8] presents a coherent survey of existing multicasting solutions for MANETs. He presents various classifications of the current multicast routing protocols, discusses their operational features, along with their advantages and limitations, and provides a comparison of their characteristics according to several distinct features and performance parameters. He make a survey on the multicast routing protocols without discussing its security aspects. Some multicast routing protocols along with their security techniques and the types of attacks they can confront are presented in [9], but the paper didn’t make a detailed comparison for resistance of multicast routing protocols against all well-known attacks.

There is a large body of work on securing mobility networks in contexts complementary to ours [10, 11, 12, 13, 14]. This includes joint encryption and error correction structure [15]. The work in [15] aims to ensure secure and robust communication in wireless sensor networks. Other recent work looks at authentication schemes with anonymity for the Global Mobility Network (GLOMONET) [16]. The authors propose a secure and efficient smart card-based user authentication scheme with anonymity for the GLOMONET. Broadcasting problem has also been explored in [17], Brian et al. in [17] define the MANET broadcasting problem as a multi-objective problem, the authors identify three broadcasting objectives: (1) max. broadcast delivery ratio; (2) max. relay energy lifetime; and (3) max. broadcast speed.

Security in multicast routing in MANETs is crucial in order to enable effective and efficient multicast-based applications. However, the unique characteristics of such networks such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology [18] pose a number of non-trivial challenges to the design of security issues. These challenges clearly make a case for building security solutions that achieve broad protection without compromising the network performance[19].

Over the last decade, several security techniques have been designed for different environments and security objectives [20], and to extend the capability of well-known ad hoc routing protocols [18],[19]. For the purpose of this paper, we classify multicast routing protocols in MANETs into two main categories: (1) Secure routing, in which security techniques are embedded within the original
design of the routing protocol, and (2) security-enhanced routing, in which security techniques are added after the routing protocol is designed.

The objective of this paper is to develop a good understanding of the various multicast routing protocols in MANETs and its capability in confronting key known attacks. Accordingly, the paper provides a survey on secure and security-enhanced multicast protocols in MANETs. To do so, the operational concepts of the main multicast routing protocols are first identified and summarized. Second, well-known attacks that threat the security of the described multicast operations are summarized and discusses. Third, we survey key security techniques used to confront various attacks, and finally we analyze the capability of the both secure and security-enhanced protocols with respect to the various known attacks identified above.

The rest of the paper is organized as follows. Section 2 presents a relevant background work, including a classification for multicast routing protocols, short description of the main types of attacks on MANETs, and brief overview about the main basic security techniques for securing the multicast routing protocols. Sections 3, 4 present summary of the main secure and security-enhanced multicast routing protocols in MANET, respectively. A categorization and comparison between security approaches against well-known types of attacks on MANET is presented in Section 5.

2. BACKGROUND

In this section, we look at relevant background work in brief, including prior work on the classification of multicast routing protocols in MANETs, the general security techniques for multicast routing protocols in MANETs, and the main attacks on routing protocols in MANETs.

2.1. Classification of Multicast Routing Protocols

Multicasting in MANETs can be implemented in the network layer, the MAC layer, and / or the application layer [8]. Accordingly, multicast routing protocols can be classified into three categories: (1) Network (IP) Layer Multicast (IPLM), (2) Application Layer Multicast (ALM) and (3) MAC Layer Multicast (MACLM).

IPLM is the most common type of multicasting used in ad-hoc networks to design efficient and reliable multicast routing protocols. It operates on network (IP) layer that require the cooperation of all nodes in the network, as the intermediate (forwarder) nodes must maintain the multicast state per group. The network layer maintains the best effort unicast datagram service compared to other types that employ other layers than network layer.

ALM, also called “overlay multicast”, is the least common type of multicasting in ad-hoc networks, as it operate at the application layer and this layer is application-depended and thus, the multicast functionality may differ from one operating system to another. However, it has very attractive features such as, the simplicity of deployment, also intermediate nodes do not have to maintain their per group state for each multicast group. Overlay multicasting can deploy the capabilities of lower-layer protocols in providing flow control, congestion control, security, or reliability according to the requirements of the application.
The third type of multicasting is the MACLM which operates on the MAC layer. It maintains the acknowledgement system to provide some sort of reliability in the peer-to-peer connections. This method requires nodes on the multicast tree (source node, destination nodes, and forwarder nodes) to buffer the multicast data packets until the feedback has been received. However, this method may cause significant end-to-end latencies in multicast data delivery especially if the source and destination are separated by a large number of hops.

Figure 2 shows various classifications of the multicast routing protocols in MANETs [8]. It illustrates the main classification dimensions for multicast routing protocols such as: multicast topology, initialization approach, routing scheme, and maintenance approach. Figure 2 shows the dependencies between the different dimensions of the multicast routing protocols, for example, shared tree based located under tree based approach which locate under multicast topology in the multicast routing protocol design considerations.

We present four classification dimensions for multicast routing protocols namely multicast topology, routing initialization approach, routing scheme, and maintenance approach. In the following, we briefly explain each of the four dimensions.

1. **Multicast Topology**: multicast topology is classified into three approaches namely tree-based, mesh-based, and stateless approach. The three approaches are described as the following:
   - **Tree-based approach**, is a very well established concept in wired networks. Most schemes for providing multicast in wired networks are either source- or shared-tree-based. Different researchers have tried to extend the tree-based approach to provide multicast in a MANET environment. A single path between source and receiver exist. This path and other paths are maintained by a general purpose node called core-node. There are two types of tree-based approach: (a) Source-Tree-based, in which each source maintains a separated tree
that contain the source node as the root of the tree and all receivers lies under this node, and (b) Shared-Tree-based, in which one tree is established in the entire network which includes all sources and receivers and in this case a core node manages the tree (act as a root to the tree).

- **Mesh-based approach**, in contrast to a tree-based approach, mesh-based multicast protocols may have multiple paths between any source and receiver pair. Existing studies show that tree-based protocols are not necessarily best suited for multicast in a MANET where network topology changes frequently. In such an environment, mesh-based protocols seem to outperform tree-based proposals due to the availability of alternative paths, which allow multicast datagrams packets to be delivered to the receivers even if links fail. In this approach, multiple paths are established in the entire network. These redundant paths are useful in link failure case and provide higher packet delivery ratio.

- **Stateless approach**, in order to minimize the effect of such problems in tree-based and mesh-based approaches, the stateless multicast approach is proposed where in source node explicitly mentions the list of destinations in the packet header. Stateless multicast focuses on small group multicast and assumes the underlying routing protocol to take care of forwarding the packet to respective destinations based on the addresses contained in the header.

2. **Routing Initialization Approach**: routing initialization can be classified into three approaches namely source-initiated, receiver-initiated, and hybrid approach. The three approaches are described as the following:

- **Source-initiated approach**, in which the multicast group construction and maintenance tasks are done by the source node. In order to initiate a new multicast group, the source node broadcast a join query message all over the network and every node wants to join this multicast group reply with join reply message.

- **Receiver-initiated approach**, in which the receiver node searches about the multicast group to join with a dedicated sources. In order to join a new multicast group, the receiver node broadcast a join query message all over the network and the source node or a core node will reply with join reply message with multicast group core route.

- **Hybrid approach**, in which it combines some features from the source initiated and receiver initiated approaches, where the multicast group construction and maintenance tasks are done either by the source node or the receiver node.

3. **Routing Scheme**: routing scheme is classified into three approaches namely table-driven, on-demand, and hybrid approach. The three approaches are described as the following:

- **Table-driven scheme** (also called “proactive”). In a network utilizing a proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain up-to-date routing information from each node to every other node. To maintain up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis, leading to relatively high overhead on the network. On the other hand, routes will always be available on request.
• **On-demand scheme (also called “reactive”).** It seeks to set up routes on-demand, if a node wants to initiate communication with a node to which it has no route, the routing protocol will try to establish such a route. Reactive multicast routing protocols have better scalability than proactive multicast routing protocols. However, when using reactive multicast routing protocols, source nodes may suffer from long delays for route searching before they can forward data packets.

• **Hybrid scheme,** which combine the proactive and reactive approaches in one approach, in order to overpass the limitations of both protocols and strength the advantages of them. An example for hybrid approach is Zone Routing Protocol (ZRP)[21] that maintains routing information for a local zone, and establishes routes on demand for destinations beyond this local neighborhood. It limits the scope of the local zone by defining a maximum hop number for the local zone.

4. **Multicast Maintenance Approaches:** multicast maintenance is classified into two approaches namely Soft-State, and Hard-State approach. The two approaches are described as the following:

• **Soft-state approach,** in which broken links maintenance process initiated periodically by flooding the network with continuous control packets to explore other routes between source and receiver. This approach has the advantage of reliability and better packet delivery ration, but it is much makes overhead over the network as it continuously flood the network with control packets.

• **Hard-state approach,** in which broken links maintenance process is established by two types namely reactive and proactive. In reactive approach, broken link recovery process is initiated only when a link breaks. The second type is proactive approach, in which routes are reconfigured before a link breaks, and this can be achieved by using local prediction techniques based on GPS or signal strength.

2.2. **Main Attacks on Multicast Routing protocols**

Compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority, lack of trust relationships between mobile nodes, ease of eavesdropping because of shared wireless medium, dynamic network topology, low bandwidth, and energy & memory constraints of mobile devices. The security issue of MANETs in group communications is even more challenging because of the involvement of multiple senders and multiple receivers.

Figure 3 shows that attacks on multicast protocols can be divided 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; (2) Multicast attacks, in which attacks are focused on the multicast operations of the protocol. These attacks are protocol dependent attacks in which are specially designed for specific protocol, i.e., not common on all multicast routing protocols, as it attack one or more internal multicast operation(s) of the protocol. For instance, in MAODV protocol [22], it attacks the multicast group establishment and maintenance.
We summarize the most common unicast attacks presented in literature on MANET, namely rushing attack, blackhole attack, neighbor attack, jellyfish attack, and denial of service attack, location disclosure, replay, wormhole, selfish and spoofing attack.

- **Rushing Attack** [23]: When source nodes flood the network with route discovery packets in order to find routes to destinations, each intermediate node processes only the first non-duplicate packet and discards any duplicate packets that arrive at a later time. A rushing attacker exploits this duplicate suppression mechanism by quickly forwarding route discovery packets in order to gain access to the forwarding group. Many demand-driven protocols which use some form of duplicate suppression in their operations, are vulnerable to rushing attacks.

- **Blackhole Attack** [24]: A blackhole attacker first needs to invade the multicast forwarding group (e.g., by implementing rushing attack) in order to intercept data packets of the multicast session. It then drops some or all data packets it receives instead of forwarding them to the next node on the routing path. This type of attack often results in very low packet delivery ratio.

- **Neighbor Attack** [24]: Upon receiving a packet, an intermediate node records its ID in the packet before forwarding the packet to the next node. An attacker, however, simply forwards the packet without recording its ID in the packet to make two nodes that are not within the communication range of each other believe that they are neighbors (i.e., one-hop away from each other), resulting in a disrupted route.

- **Jellyfish Attack** [24]: A jellyfish attacker first needs to intrude into the multicast forwarding group. It then delays data packets unnecessarily for some amount of time before forwarding
them. This results in significantly high end-to-end delay and thus degrades the performance of real-time applications. Jellyfish attacks affect the packet end-to-end delay and the delay jitter, but not the packet delivery ratio or the throughput.

- **Denial of service (DoS) Attack** [25]: DoS is the degradation or prevention of legitimate use of network resources. MANET is particularly vulnerable to DoS attacks due to its features of open medium, dynamic changing topology, cooperative algorithms, decentralization of the protocols, and lack of a clear line of defense is a growing problem in networks today.

- **Location Disclosure Attack** [26]: Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques, or with simpler probing and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network.

- **Replay Attack** [24]: It is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

- **Wormhole Attack** [27]: The wormhole attack is one of the most powerful presented in MANETs since it involves the cooperation between two malicious nodes that participate in the network. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers.

- **Selfish Attack** [24]: It is a form of internal attacks, in which one or several nodes want to preserve its own resources while using the services of others and consuming their resources, such misbehaving nodes participate in the route discovery and maintenance phase but refuse to forward data packets, which degrades routing performance.

- **Spoofing Attack** [24]: The attacker must impersonate another illegitimate node by falsifying data and thereby gaining an illegitimate access to network resources. The attacker must monitor the packets sent from source to destination and then guess the sequence number of the packets. Then the attacker injects his own packets, claiming to have the address of the source node.

We summarize some of multicast attacks presented in literature on MAODV protocol [28], [29], namely MACT(J)-MTF attack, MACT(P)-PART attack, RREP(J)-PART attack, Group Leader Selection (GLS) attack, False link breakage (FLB) attack and Group leader pruning (GLP) attack.

- **Multicast Activation includes Join flag - Multicast Tree Formation (MACT(J)-MTF) attack** [28]. A malicious node can launch attack against link activation operation of MAODV protocol by broadcasting a RREQ message with ‘J’ flag set in order to join the multicast group, it may receive multiple RREPs in response to its RREQ. The malicious node doesn’t select the best 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 (i.e., a mesh topology is created instead of tree topology).
- **Multicast Activation includes Prune flag - Multicast Tree Partition (MACT(P)-PART) attack** [28]. A malicious node can launch attack against tree pruning operation of MAODV protocol by impersonating a group member and broadcasting a MACT message with ‘P’ flag set to indicate that this group member wants to prune itself. If the 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.

- **Route Reply includes Join flag - Multicast Tree Partition (RREP(J)-PART) attack** [28]. A malicious node can launch attack against link repair operation of MAODV protocol by partitioning the multicast tree. When a node’s link to its neighbor node in the multicast tree breaks, the malicious node may respond with a RREP message 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.

- **Group Leader Selection (GLS) attack** [29]. A malicious node can launch attack against group leader selection operation by deceiving tree nodes to become a group leader. The malicious node broadcasts a GRPH message (with hop count less than the existing group leader’s hop count) to inform tree nodes that it is now the group leader. 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.

- **False link breakage (FLB) attack** [29]. 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, 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.

- **Group leader pruning (GLP) attack** [29]. 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, when a downstream node receives a MACT message with ’P’ flag set from upstream node, it propagates RREQ message through 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.

### 2.3. Security Techniques for Multicast Routing Protocols in MANETs

In this sub-section, we discuss some of the basic security techniques in literature for MANET, in which secure and security-enhanced multicast routing protocols use it to build their security structure. The presented techniques are asymmetric cryptography key, symmetric cryptography key, certificate server, digital signature, hash message authentication code (HMAC), and hash chain functions.
1. **Asymmetric Cryptography Key** [30]. In which each node has a public/private key pair that can be appended to a message as a security signature. It does not require a secure initial exchange of one or more secret keys to both sender and receiver. The asymmetric key algorithms are used to create a mathematically related key pair; a secret private key and a published public key. Use of these keys allows protection of the authenticity of a message by creating a digital signature of a message using the private key, which can be verified using the public key.

2. **Symmetric Cryptography Key** [31]. It uses a nonce or a shared key between each pair of nodes. The shared keys are used to generate keyed-hash message authentication codes, while the nonce is used by one-way hash functions in order to generate hash chains, or hash tree chains. Symmetric cryptography uses trivially related, often identical, cryptographic keys for both decryption and encryption. Any member node that has the key can use it to encrypt and decrypt data. Symmetric cryptography algorithms are typically fast and are suitable for processing large streams of data.

3. **Certificate Server** [30]. It is based on asymmetric cryptography mechanism, in which every node in the network signed by a Certification Authority (CA) server, which considered the key identity for the node to participate in the network operations. A certificate signed by CA can be readily verified by well-know system public key. The authority of CA is distributed among many network nodes, called servers, to minimize the chance of a single CA being compromised. All the nodes certificates are divided into (n) shares and distributed to server nodes before network formation. If a node requires other nodes public key, it requests to server nodes which generate their partial signatures individually.

4. **Digital Signature** [31]. It is a mathematical scheme for demonstrating the authenticity of packets. It is based on asymmetric key cryptography. A valid digital signature gives the message receiver a good reason to believe that the message was created by a known sender, and that it was not altered in transit. A digital signature scheme typically consists of three algorithms; key generation, signing, and signature verifying algorithm. A digital signature can be verified by any node given that it knows the public key of the signing node. This makes digital signature scalable to large numbers of receivers.

5. **Hash Message Authentication Code (HMAC)** [32]. It is based on symmetric cryptography mechanism, which is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key. It can be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of HMAC depends on the properties of the underlying hash function.

6. **Hash Chain Functions** [33]. It is based on symmetric key cryptography, which involves much less computation overhead in signing, decrypting and verifying, and encrypting operations. Hash chain is a method to produce many one-time keys from a single key. Hash chain is built on a one-way hash function like a normal hash function. A traditional approach for key distribution is used. A trusted CA has to sign public-key certificates for each node; each node can then use its public-key to sign new a hash chain element for itself.
3. SECURE MULTICAST ROUTING PROTOCOLS IN MANETS

This section describes the most common secure multicast routing protocols in MANETs, in which security techniques are embedded within the original design of the routing protocol. The protocols described in this section are: SMGMP [34], BSMR [35], SEAMAN [36], SORB [37] and ALMA [38]. For each protocol, we present a brief description, key limitation, and security challenges and evaluation.

In Table I, we summarize the presented secure multicast routing protocols in terms of various characteristics such as, security-extended protocol, main objectives, implementation method, performance metrics and overhead metrics. Table II presents a comprehensive representation of the secure multicast routing protocols classification, that provides a tabular view of routing scheme, initialization of multicast connectivity, multicast topology, and multicast topology maintenance.

Table III gives a summary of the secure multicast routing protocols and security techniques they use. Almost all presented protocols adopt more than one security technique in order to achieve different secure objectives. Most of them use either asymmetric cryptography key or symmetric cryptography key to generate security keys to authenticate control messages and / or data packets. For securing mutable data certificates, digital signatures or HMACs can be used for authentication and integrity.

3.1. Secure Multicast Group Management Protocol (SMGMP)

Protocol Description. SMGMP [34] is a secure multicast group management protocol that address some problems specific to ad hoc networks such as mobility, unreliable links, and cost of multi-hop communication. SMGMP do not address the problem of multicast routing of data information, but it assumes that the multicast data can take the same path as the security traffic or a different path. Since SMGMP’s main focus is on reducing the communication cost, multicast groups members participate in the security of the multicast group. The main idea of SMGMP is to have group members actively participate to the security of the multicast group (i.e., the group security is distributed among the group members). The proposed idea reduces the communication and computation load on the multicast source. Authorized group members are given a service right certificate that allows them to verify that a node is authorized to join the multicast group.

Discussion. SMGMP proposes some security assumptions such as the nodes with a valid service right certificate should only be able to access the data stream, and nodes should not be able to receive any data after the revocation of their certificate. SMGMP’s basic scheme for secure multicasting is based on maintaining a physical security tree of the group members. Nodes that want to join the multicast group should discover the (best-closest) tree node and attach to the multcat group through it. The secure multicast tree is used to securely forward the group key to authorized members. Service right certificates allow joining nodes to prove that it is authorized to access some service, and to become part of the multicast group. SMGMP use a classical public key authentication protocol based on certificates for authenticating nodes.
Table I. Secured Multicast Routing Protocols Features, [PDR: Packet Delivery Ratio]

<table>
<thead>
<tr>
<th>Protocol Name</th>
<th>Objectives</th>
<th>Design Considerations</th>
<th>Performance Evaluation</th>
<th>Performance Metrics</th>
<th>Overhead Metrics</th>
</tr>
</thead>
</table>
| SMGMP [34]    | • Secure multicast data streams  
• Group members authentication  
• Data integrity | • Group members participate to the security of the multicast group.  
• Only the nodes with a valid certificate should be able to access the data. | NS-2 Simulator | Average Delay | PktxHop: Total number of control packets X Number of hops traveled |
| BSMR [35]     | • Mitigates Byzantine attacks  
• Withstands insider attacks from colluding adversaries | • Software-based solution and does not require additional or specialized hardware.  
• Nodes are not required to be equipped with additional hardware | NS-2 Simulator | PDR | Additional Packets Transmitted (packets/second) |
| SEAMAN [36]   | • Provides foreigner detection mechanism for hosts and networks  
• Authentication, confidentiality and anonymity of MANETs | • Detection mechanism for new joining nodes  
• Provides frame encryption scheme to encrypt all MANET traffic | Realized as a combination of WNet [39], MIKE [40] and MASK [41] protocols | — | — |
| SORB [37]     | • Provides resilience against Byzantine attacks in grid form of multicast groups.  
• Identifies and avoid adversarial links  
• Efficient authentication for nodes | • Considers a three-level trust model that captures the interactions between nodes  
• Considers communication between multiple multicast groups | Theoretical Implementation | — | — |
| ALMA [38]     | • Focuses on securing the multicast infrastructure  
• Offers confidentiality, authenticity and integrity of both user traffic and control messages | • Avoids the use of complex protocols for group key management.  
• Uses application layer programs for mitigating application threats such as hacking | GloMosim Simulator | PDR, Goodput and Maximum logical degree | Multicast tree cost and stress of a physical links |

Table II. Secured Multicast Routing Protocols Classification

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Hybrid</th>
<th>Reactive</th>
<th>Proactive</th>
<th>Multicast topology</th>
<th>Initialization approach</th>
<th>Maintenance approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMGMP [34]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Tree, Mesh</td>
<td>Receiver</td>
<td>Hard state ✓ Soft state ✓</td>
</tr>
<tr>
<td>BSMR [35]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Mesh</td>
<td>Source</td>
<td>✓</td>
</tr>
<tr>
<td>SEAMAN [36]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Tree</td>
<td>Source</td>
<td>✓</td>
</tr>
<tr>
<td>SORB [37]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Mesh</td>
<td>Source</td>
<td>✓</td>
</tr>
<tr>
<td>ALMA [38]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Mesh</td>
<td>Source</td>
<td>✓</td>
</tr>
</tbody>
</table>

3.2. Byzantine-Resilient Secure Multicast Routing (BSMR) Protocol

**Protocol Description.** BSMR [35] is an tree-based on-demand multicast protocol for multi-hop wireless networks that designed to be a attack-resilient multicast routing protocol. BSMR relies on general mechanisms to mitigate Byzantine attacks (flood rushing, black hole, and wormhole).
Table III. Basic Security Techniques for Secured Multicast Routing Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Asymmetric Cryptography Key</th>
<th>Symmetric Cryptography Key</th>
<th>Certificate Server</th>
<th>Digital Signature</th>
<th>HMAC</th>
<th>Hash Chain Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMGMP [34]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>BSMR [35]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SEAMAN [36]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SORB [37]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ALMA [38]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

BSMR identifies and avoids adversarial links based on a reliability metric associated with each link and capturing adversarial behavior. BSMR ensures that multicast data is delivered from the source to the members of the multicast group, even in the presence of Byzantine attackers, as long as the group members are reachable through non-adversarial paths and a non-adversarial path exists between a new member and a node in the multicast tree. BSMR’s additional overhead consists only of periodical packets and of occasional route discovery in case a link breaks due to mobility.

Discussion. BSMR uses authentication framework to protect the network from external attacks against the creation and maintenance of the multicast tree. The proposed framework prevents unauthorized nodes from joining the multicast tree. Each node authorized to join the network has a pair of public/private keys and a node certificate that binds its public key to its IP address. Each node authorized to join a multicast group has an additional group certificate that binds its public key and IP address to the IP address of the multicast group. BSMR uses a selective data forwarding detection mechanism that relies on a reliability metric capturing adversarial behavior. Nodes determine the reliability of links by comparing the perceived data rate with the one advertised by the source. Adversarial links are avoided during the route discovery phase.


Protocol Description. SEAMAN [36] is an efficient multicast multi-hop ad hoc routing protocol that provide a high level of security while benefiting from the advantages of MANETs. It detects and authenticates single foreign hosts and foreign networks that want to join a secured MANET. SEAMAN offers external anonymity, confidentiality, authenticity and integrity of both user traffic and routing messages, while providing effective mechanisms against internal attackers. SEAMAN provide a frame encryption scheme that uses a common key to encrypt all MANET traffic, and a key management system to dynamically generate and update the common key. SEAMAN in uses MAC layer forwarding, as it handles every frame sent over the wireless interface. It uses a dynamic MANET key to encrypt every frame before delivering it to the wireless interface.

Discussion. The two main aspects of security proposed by SEAMAN are the anonymity of MANET nodes and the encryption of the whole link layer with a dynamic key. External anonymity is guaranteed in SEAMAN by the use of perfect pseudonyms in the authentication part of the protocol. The key management subsystem establishes and maintains a common MANET key even if members join or leave the MANET. All data leaving a MANET node is encrypted with the MANET key, including the complete routing management traffic. Authenticity and integrity is ensured by the HMAC appended to every message. SEAMAN can react even on internal security threats. The reaction of SEAMAN on an internal attacker is to publish the compromised nodes symmetric key,
revoke its certificate and update the MANET key. Now it is impossible for an internal attacker or a compromised node to reveal the identities of other nodes.

3.4. Secure On-Demand Resilient to Byzantine Multicast (SORB) protocol

**Protocol Description.** SORB [37] is a secure on-demand multicast routing protocol for multi-hop wireless networks that provides resilience against Byzantine attacks such as flood rushing [23] and blackhole [24] attack. SORB assumes multihop wireless network model where nodes participate in the data forwarding process for other nodes. SORB protect the network from external attacks against the creation and maintenance of the multicast tree and prevents unauthorized nodes to be part of the multicast tree. SORB uses multi-path routing to prevent a malicious node from selectively dropping data. It ensures that multicast data is delivered from the source to the members of the multicast group, even in the presence of Byzantine attackers, as long as the group members are reachable through non-adversarial path.

**Discussion.** SORB provides authentication framework in order to prevent unauthorized nodes to be part of the multicast group. Each node authorized to join the network has a pair of public/private keys and node certificate that binds its public key to its IP address. SORB proposes hop count authentication to prevent tree nodes from claiming to be at a smaller hop distance from the group leader than they actually are, SORB uses a technique based on a hash chain. SORB prevents unauthorized node from sending and receiving control messages using efficient authentication scheme, as it uses pair wise keys shared between neighbor nodes that exchange control messages.

3.5. Application Layer Multicast Algorithm (ALMA)

**Protocol Description.** ALMA [38] is a receiver-driven overlay multicast application layer protocol. ALMA constructs an overlay multicast tree in a dynamic, decentralized and incremental way. ALMA is flexible, and thus, it can satisfy the performance goals and the needs of a wide range of applications. ALMA has the advantages of an application layer protocol such as simplicity of deployment, and independence from lower layer protocols. It has the capability of exploiting features such as reliability and security that may be provided by the lower layers. ALMA creates a logical multicast logical mesh tree between the multicast members, but a tree induces less maintenance overhead. A joining node joins the group by sending join messages to possibly multiple existing members. A parent group member responds to this message and take that node as a child node. ALMA uses soft state approach to deal with failures and partitions.

**Discussion.** ALMA provides security according to the needs of applications, and it proposes secure multicast infrastructure. In addition, secure group communications are reduced to secure unicast communications, which avoid the use of complex protocols for group key management. ALMA offer to the applications running on the application layer the confidentiality, authenticity and integrity of both user traffic and control messages, while providing effective mechanisms against against unauthorized access and attacks. ALMA work to protect the network from application attacks including hacking, cross-site scripting, and parameter tampering, as well as network attacks as spoofing, selfish, replay, and denial of services attack.
4. SECURITY-ENHANCED MULTICAST ROUTING PROTOCOLS IN MANETS

This section describes the most common security-enhanced multicast routing protocols in MANETs, which extend none-secured multicast routing protocols in MANET by adding security techniques after the design of the original protocols. The protocols described in this section are: R-ODMRP [42], SMRMN [43], DIPLOMA [44], CBMT [45], SMMARP [46], SE-MAODV [28] and EC-MAODV[29]. For each protocol, we present a brief description, key limitation and security challenges and evaluation.

In Table IV, we summarizes the presented security-enhanced multicast routing protocols in terms of various characteristics such as, security-extended protocol, main objectives, design considerations, implementation method, performance metrics and overhead metrics. Table V presents a comprehensive representation of the security-enhanced multicast routing protocols classification, that provides a tabular view of routing scheme, initialization of multicast connectivity, multicast topology, and multicast topology maintenance. Table VI gives a summary of the security-enhanced multicast routing protocols and security techniques they use.

4.1. Reliable On-Demand Multicast Routing Protocol (R-ODMRP)

Protocol Description. R-ODMRP [42] is a secure extension to ODMRP (On-Demand Multicast Routing Protocol) [47]. R-ODMRP is proposed for preferable throughput and especially designed for MANET, which includes packet acknowledgement, lost packet recovery and secure authentication. R-ODMRP constructs the multicast routing based on clustering approach, which uses the concept of forwarding group, and builds multicast mesh which is maintained through soft state and gains high performance. R-ODMRP builds forwarding mesh for each multicast group, flexible soft-state maintenance, mobility prediction and QoS (Quality of Service) scheduling. The PDR (Packet Delivery Ratio) of R-ODMRP is higher than that of ODMRP because the cluster based mesh improves the reliability of packet delivery through distributed packet acknowledgement and lost packet recovery. R-ODMRP needs to set up cluster based mesh and key exchanging, its overhead increases with the load and gets heavier at first.

Discussion. R-ODMRP authenticates the consistency of multicast source and receivers depending on local security strategy. Each node has asymmetric key, a public key and a private key. Any node can exchange public key with neighbors through HELLO message. In order to decrease the multicast delay and complexity of authentication, authors design a cluster based authentication strategy. After a cluster head is voted, the cluster key distributes with the cooperation of neighbors signature and exchanged through key message after HELLO message. With cluster based authentication strategy, R-ODMRP ensures the following: the multicast packets are from the legal source, packets are not interrupted during the delivery, receivers are legal group members.
Table IV. Security-Enhanced Multicast Routing Protocols Features, [PDR: Packet Delivery Ratio]

<table>
<thead>
<tr>
<th>Protocol Name</th>
<th>Security-Extended Protocol</th>
<th>Objectives</th>
<th>Design Considerations</th>
<th>Performance Evaluation</th>
<th>Performance Metrics</th>
<th>Overhead Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-ODMRP [42]</td>
<td>ODMRP [47]</td>
<td>• Presents a reliable multicast routing protocol based on ODMRP</td>
<td>• Authenticates the consistency of multicast source and receivers depending on local security strategy</td>
<td>NS2 Simulator and MATLAB</td>
<td>PDR and Average Delay</td>
<td>Control Byte Overhead</td>
</tr>
<tr>
<td>SMRMN [43]</td>
<td>MAODV [22]</td>
<td>• Proposes secure multicast routing based on MAODV protocol</td>
<td>• Addresses the problem of securely building and maintaining multicast trees in MANETs</td>
<td>Theoretical Implementation</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>DIPLOMA [44]</td>
<td>ODMRP [47], PIM-SM [48]</td>
<td>• Proposes secure multicast traffic based on ODMRP and PIM-SM protocols</td>
<td>• Enforce trust relationships between mobile nodes through a distributed policy enforcement scheme</td>
<td>Orbit lab MANET testbed using Linux systems running Debian Linux</td>
<td>Multicast Throughput, Packet Loss Rate, and Packet Inter Arrival Times</td>
<td>—</td>
</tr>
<tr>
<td>CBMT [45]</td>
<td>MDSDV [49]</td>
<td>• Presents a new approach of clustering algorithm for efficient multicast key distribution in MDSDV protocol</td>
<td>• Uses distributed key-agreement scheme</td>
<td>NS2 Simulator</td>
<td>End to End Delay, Energy Consumption, Key Delivery Ratio, and Packet Drop Ratio</td>
<td>—</td>
</tr>
<tr>
<td>SMMARP [46]</td>
<td>MMARP [50]</td>
<td>• Proposes secure multicast routing based on MMARP protocol</td>
<td>• Uses public/private key pair in each node in the network</td>
<td>Theoretical Implementation</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>SE-MAODV [28]</td>
<td>MAODV [22]</td>
<td>• Propose an authentication framework for mitigating multicast attacks on MAODV protocol</td>
<td>• Each authorized node possesses a public/private key pair and group certificate</td>
<td>NS2 Simulator</td>
<td>PDR and Total Packets Transmitted</td>
<td>Control Byte Overhead</td>
</tr>
<tr>
<td>EC-MAODV [29]</td>
<td>MAODV [22]</td>
<td>• Proposes security countermeasures for securing MAODV against multicast attacks</td>
<td>• Uses control messages authentication and group certificate countermeasures</td>
<td>QualNet Simulator</td>
<td>PDR</td>
<td>Control Byte Overhead</td>
</tr>
</tbody>
</table>
Table V. Security-Enhanced Multicast Routing Protocols Classification

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Routing Scheme</th>
<th>Multicast topology</th>
<th>Initialization approach</th>
<th>Maintenance approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-ODMRP [42]</td>
<td>Hybrid</td>
<td>Reactive</td>
<td>Tree</td>
<td></td>
</tr>
<tr>
<td>SMRMN [43]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DIPLOMA [44]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>CBMT [45]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SMMARP [46]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SE-MAODV [28]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>EC-MAODV [29]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Table VI. Basic Security Techniques for Security-Enhanced Multicast Routing Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Asymmetric Cryptography Key</th>
<th>Symmetric Cryptography Key</th>
<th>Certificate Server</th>
<th>Digital Signature</th>
<th>HMAC</th>
<th>Hash Chain Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>R-ODMRP [42]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMRMN [43]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIPLOMA [44]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CBMT [45]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMMARP [46]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SE-MAODV [28]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EC-MAODV [29]</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.2. Secure Multicast Routing with Misbehaving Nodes (SMRMN) Protocol

Protocol Description. SMRMN [43] is a secure extension to the well-known MAODV (Multicast Adhoc On-demand Distance Vivtor) routing protocol [22]. Unlink MAODV, SMRMN does not rely on the use of sequence numbers and hop counts. Only control messages join RREQ (Route Request) and repair RREQ messages are used to discover routes to their destination. The protocol does not guarantee to find the shortest path but offers a good path which delivers the message to the destination with the least delay. SMRMN addresses the problem of misbehaving nodes which are authorized but compromised by attackers. The protocol handel unauthorized nodes, as well as misbehaving nodes. SMRMN addresses the problem of control attacks on multicast trees. Moreover, the protocol guards against various passive/active control attacks from both outsiders and insiders.

Discussion. SMRMN proposes security techniques for securing the exchange of multicast data packets and control packets, in addition to make it possible for every legitimate node to join or leave an existing group securely. SMRMN uses timestamps to verify the freshness of control messages, and uses IPSEC [51] to authenticate the IP header. Any attempts to modify or replay control messages will be detected by the signature and timestamp mechanisms, respectively. Control messages can be generated only by a legitimate group member and, therefore, only authorized nodes can participate in the group, and only legitimate group member can reply on control messages. Every authorized node has its public and private key pair and knows the public key of the certificate authority in order to authenticate control packets as well as data packets.

4.3. DIPLOMA

Protocol Description. DIPLOMA [44] is a secure extension to both multicast routing protocols ODMRP (On Demand Multicast Routing Protocol) [47] and PIM-SM (Protocol Independent Multicasting Spare Mode) [48] in order to provide a unified solution for both receiver access control and sender access control for MANETs. DIPLOMA is a deny-by-default architecture that enforces trust relationships and traffic accountability between mobile nodes through a distributed...
policy enforcement scheme for MANETs. DIPLOMA prevents unauthorized senders from sending control messages to a multicast group, as well as preventing unauthorized receivers from joining the multicast group. It works on protecting the end-host resources and the save network bandwidth. DIPLOMA modified the well-known multicast protocols such as ODMRP and PIM-SM in order to incorporate with DIPLOMA. The authors showed impact of the proposed scheme is minimal on throughput, packet loss, and packet inter-arrival times.

Discussion. DIPLOMA's main goal is to protect network resources and the multicast traffic from Denial of Service (DoS) attack [25], and to enforce access control rules in the absence of a fixed topology of MANET environment. Authors assume MANET environments where the attacker may insider node or a malicious external node that might want to participate in the MANET. All network capabilities are signed by the group controller and are verifiable by all nodes, attackers cannot generate their own valid capabilities, unless the group controller is compromised. DIPLOMA appends on every transmitted packet a transaction identifier, a public key, and a packet signature based on that public key. The packet signatures for a block of packets consist of RSA signature for the first packet and SHA-1 hashes for the remaining packets. The RSA signature is verifiable with the key sent in the capability establishment phase. The SHA-1 hashes are integrity protected by including them in the first packet. Since all individual packets are signed, the attacker cannot tamper the transmitted multicast traffic.

4.4. Cluster-Based Multicast Tree (CBMT)

Protocol Description. CBMT [45] uses dynamic clustering scheme with MDSDV (Multicast Destination Sequenced Distance Vector) routing protocol [49], which used it to elect the local controllers of the clusters and updates periodically as the node joins and leaves the cluster. CBMT is an efficient cluster-based multicast tree algorithm for secure multicast key distribution in MANETs by overcoming issues of multicast key management requirements. The proposed scheme overcomes 1-affects-n phenomenon, reduces average latency and energy consumption and achieves reliability, while exhibiting low packet drop rate with high key delivery ratio. CBMT improves the performance in terms of QoS metrics as node increases by using an approach of efficient cluster based multicast tree algorithm for secure multicast communication.

Discussion. CBMT assumes some security requirements such as the following: Group members left the group should not have access to any future key. This ensures that a group member cannot decrypt data after it leaves the group. A new joining node should not have access to any old key. This ensures that a member cannot decrypt data sent before it joins the group. CBMT proposes non-group confidentiality, in which members that not a part of the multicast group, should not have access to any key that can decrypt any multicast data sent to the group. CBMT uses distributed key-agreement scheme, in which group members cooperate to establish a group key. This improves the reliability of the overall system and reduces the bottlenecks in the network.

4.5. Secure Multicast MANet Routing Protocol (SMMARP)

Protocol Description. SMMARP [46] is a secure extension to MMARP (Multicast MANet Routing Protocol) [50] to protect the protocol against spoofing and forging attacks, based on cryptographically generated addresses and digital signatures. MMARP uses a hybrid approach to
build a distribution mesh. Routes among ad hoc nodes are established on-demand, whereas routes towards nodes in the fixed network are maintained proactively. When a member wants to send data, it periodically broadcasts a MMARP SOURCE message which is flooded within the entire network to update the state of intermediate nodes as well as the multicast routes. When this message arrives at a receiver, it broadcasts a MMARP JOIN message including the IP address of the previous hop towards the sender. When a member detects its IP address in the JOIN message, it recognizes that it is in the path between the source and the destination. It then activates its multicast forwarder flag for the group. Once the mesh is established, data packets addressed to a certain multicast group are only propagated by ad hoc nodes which have their multicast forwarder flag active for that group.

Discussion. MMARP protocol was initially designed without considering security vulnerabilities such as impersonalization of a node by forging MMARP SOURCE or MMARP JOIN messages, and the payload of any MMARP message may be forged when forwarded. SMMARP proposes two mechanisms to secure the MMARP operation: digital signatures to prevent the forging of messages, and cryptographically generated addresses to prevent address spoofing. Both solutions are based in asymmetric cryptography, so that each node needs a public/private key pair. Digital signatures are used to protect the integrity of both non-mutable and mutable fields of MMARP messages. The signatures are calculated using the private key of the nodes, and the Cryptographically Generated Addresses (CGA) is generated using the public key of the nodes. If an attacker wants to take a CGA created by someone else and send signed messages that appear to come from the owner of that address, it needs to know the private key of the owner of the address. Thus, the authentication of the node and the integrity of the messages are guaranteed.

4.6. Security Enhanced Multicast Adhoc On-demand Distance Victor (SE-MAODV) protocol

Protocol Description. SE-MAODV [28] is a secure extension to MAODV (Multicast Adhoc On-demand Distance Victor) protocol [22] to protect it from multicast attacks that targets its functional multicast operations. Authors assess the vulnerability of MAODV to attacks launched by both insider and outsider nodes, and identify attacks on multicast tree formation and maintenance that have no counterpart in unicast routing protocols. The identified attacks can result in a significant degradation in the performance of MAODV. Accordingly, SE-MAODV proposes an authentication framework that can be used for preventing or mitigating the security attacks on MAODV. Attacks on MAODV are divided into two categories: attacks on route discovery, and attacks on multicast tree maintenance. The goal of these attacks is either to create a partition in the multicast tree or to build an energy inefficient multicast tree. in other words, these attacks can disrupt the normal operation of MAODV to a large extent

Discussion. SE-MAODV proposes the use of an authentication framework in which nodes need the appropriate credentials to participate in the MAODV protocol as a group member or tree node. The routing control messages exchanged between nodes are augmented to include additional fields that allow the receiving node to verify the authenticity of the message. Each authorized node in the network possesses a public/private key pair and a certificate signed by a Certification Authority (CA) called node certificate, which can be verified by all nodes. A group member has an additional group membership certificate that proves that the certificate holder belongs to a particular multicast group. A node on the multicast tree establishes pairwise shared keys with each of its immediate neighbors.
This can be done using the public keys of the two nodes. The Group Hello packets broadcast by a group leader are digitally signed for authentication. In addition, SE-MAODV secures tree Key dissemination, and authenticate the group leader hop count using one-way hash chains.

4.7. Efficient Countermeasures for Multicast Adhoc On-demand Distance Victor (EC-MAODV) protocol

Protocol Description. EC-MAODV [29] proposes security countermeasures for securing MAODV [22] against multicast attacks in order to guarantee the integrity and authentication without degradation in the performance of the protocol. Authors 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. For each attack, authors 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 under the identified attacks.

Discussion. EC-MAODV proposes two security countermeasures for securing MAODV against the identified attacks, namely control messages authentication and group certificate. LHAP is used to authenticate the control packets (RREQ, RREP, GRPH, MACT), in which the MAODV’s functional operations uses to perform its routing operations. Any control packets from unauthorized nodes are dropped, thus preventing them from propagating through the network. TESLA is used in creating the group membership certificate. 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. Every legitimate group member can verify the correctness of this certificate. If an intermediate group member fails to verify the control message, it will drop it.

5. SUMMARY

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. Known protocols and techniques for multicast routing, cryptography, and protection and attack detection that are used in conventional wired and wireless networks can be difficult to apply in MANETs. Consequently, substantial research efforts over the last decade have been focused on developing and implementing routing protocols and security techniques that better suite the nature of MANETs. Depending on whether security is built-in or added, two categorizes of multicast routing protocols are identified: secure and security-enhanced routing protocols, respectively.

This paper presents a survey on secure and security-enhanced multicast routing protocols. The capability of both secure and secured protocols along with their security techniques are summarized against various network attacks.
Table VII. Secure and Security-Enhanced Multicast Routing Protocols Against Attacks, [NA: Not Applicable, U: Unknown]

<table>
<thead>
<tr>
<th>Attack</th>
<th>Secure Multicast Protocol Name</th>
<th>Security-Enhanced Multicast Protocol Name</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SMG-MP</td>
<td>BS-MR</td>
<td></td>
</tr>
<tr>
<td>Rushing</td>
<td>✓</td>
<td>✓</td>
<td>U</td>
</tr>
<tr>
<td>Blackhole</td>
<td>✓</td>
<td>✓</td>
<td>U</td>
</tr>
<tr>
<td>Neighbor</td>
<td>✓</td>
<td>✓</td>
<td>U</td>
</tr>
<tr>
<td>Jellyfish</td>
<td>✓</td>
<td>✓</td>
<td>U</td>
</tr>
<tr>
<td>DoS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Location Dis.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Replay</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Wormhole</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Selfish</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Spoofing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MACT(J)-MTF</td>
<td>NA</td>
<td>U</td>
<td>NA</td>
</tr>
<tr>
<td>MACT(P)-PART</td>
<td>NA</td>
<td>U</td>
<td>NA</td>
</tr>
<tr>
<td>RREP(J)-PART</td>
<td>NA</td>
<td>U</td>
<td>NA</td>
</tr>
<tr>
<td>GLS</td>
<td>NA</td>
<td>U</td>
<td>NA</td>
</tr>
<tr>
<td>FLB</td>
<td>NA</td>
<td>U</td>
<td>NA</td>
</tr>
<tr>
<td>GLP</td>
<td>NA</td>
<td>U</td>
<td>NA</td>
</tr>
<tr>
<td>Total</td>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

Table VII gives a summary for the various multicast routing protocols and the attacks that each can confront. Each cell in Table VII can take one of the following four states:

- **Confronted**: The attack is applicable and can be confronted by the protocol, represented in Table VII by (√).
- **Not Confronted**: The attack is applicable on the and can’t be confronted by the protocol, represented in Table VII by empty cell.
- **Not Applicable**: The attack is not applicable on the protocol, represented in Table VII by (NA).
- **Unknown**: The attack is applicable on the protocol; however, it is unknown whether the protocol can confront the attack or not. Further studies are needed in order to determine the capability of the protocol to confront the attack. This state is represented in Table VII by (U).

Table VIII gives a summary of secure and security-enhanced multicast routing protocols based on the classifications presented in Section 2.1 against attacks. Each cell in the table gives the set of protocols, if any, that can confront a given attack.

Based on Tables VII and VIII, the key findings of this survey can be summarized as follows:

- Few multicast routing protocols have built-in security techniques (i.e., secure multicast protocols) compared to security-enhanced multicast routing protocols. However, it is well known that considering security issue early in the design of the protocol can lead to optimized and efficient routing protocols.
- For any given attack, there always exists a suitable reactive and/or tree-based routing protocol that can confront this attack.
- There is no proactive or mesh-based multicast can confront rushing, blackhole, and jellyfish attacks.
<table>
<thead>
<tr>
<th>Attack</th>
<th>Hybrid</th>
<th>Routing Scheme</th>
<th>Multicast topology</th>
<th>Initialization approach</th>
<th>Maintenance approach</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hybrid</td>
<td>Reactive</td>
<td>Proactive</td>
<td>Tree based</td>
<td>Mesh based</td>
</tr>
<tr>
<td>Rushing</td>
<td>BSMR, SORB</td>
<td>BSMR, SORB</td>
<td>BSMR, SORB</td>
<td>BSMR, SORB</td>
<td>BSMR, SORB</td>
</tr>
<tr>
<td>Blackhole</td>
<td>SMMA-RP</td>
<td>BSMR, SORB</td>
<td>BSMR, SORB, SMMARP</td>
<td>BSMR, SORB, SMMARP</td>
<td>BSMR, SORB, SMMARP</td>
</tr>
<tr>
<td>Neighbor</td>
<td>SMGMP, R-ODMRP</td>
<td>SMGMP</td>
<td>R-ODMRP</td>
<td>SMGMP, R-ODMRP</td>
<td>SMGMP, R-ODMRP</td>
</tr>
<tr>
<td>Jellyfish</td>
<td>BSMR, SORB</td>
<td>BSMR, SORB</td>
<td>BSMR, SORB</td>
<td>BSMR, SORB</td>
<td>BSMR, SORB</td>
</tr>
<tr>
<td>DoS</td>
<td>SMGMP, SMRMN, DIPLOMA</td>
<td>SEAMAN, ALMA, CBMT</td>
<td>SEAMAN, ALMA, CBMT</td>
<td>SEAMAN, ALMA, CBMT</td>
<td>SEAMAN, ALMA, CBMT</td>
</tr>
<tr>
<td>Location Disclose</td>
<td>R-ODMRP</td>
<td>SEAMAN, CBMT</td>
<td>SEAMAN, CBMT</td>
<td>SEAMAN, CBMT</td>
<td>SEAMAN, CBMT</td>
</tr>
<tr>
<td>Replay</td>
<td>SMRMN</td>
<td>SEAMAN, ALMA</td>
<td>SEAMAN, ALMA, SMRMN</td>
<td>ALMA, SMRMN</td>
<td>SEAMAN, SMRMN</td>
</tr>
<tr>
<td>Wormhole</td>
<td>SMMA-RP</td>
<td>BSMR, SORB</td>
<td>BSMR, SORB</td>
<td>SMMA-RP</td>
<td>SMMARP</td>
</tr>
<tr>
<td>Selfish</td>
<td>SEAMAN, ALMA</td>
<td>SEAMAN, ALMA</td>
<td>SEAMAN, ALMA</td>
<td>SEAMAN, ALMA</td>
<td>SEAMAN, ALMA</td>
</tr>
<tr>
<td>Spooing</td>
<td>SMRMN, DIPLOMA</td>
<td>SEAMAN, ALMA</td>
<td>SEAMAN, ALMA, SMRMN</td>
<td>DIPLOMA</td>
<td>SEAMAN, SMRMN</td>
</tr>
<tr>
<td>MACT(J)-MTF</td>
<td>SE-MAODV</td>
<td>SE-MAODV</td>
<td>SE-MAODV</td>
<td>SE-MAODV</td>
<td>SE-MAODV</td>
</tr>
<tr>
<td>MACT(P)-PART</td>
<td>SE-MAODV</td>
<td>SE-MAODV</td>
<td>SE-MAODV</td>
<td>SE-MAODV</td>
<td>SE-MAODV</td>
</tr>
<tr>
<td>RREP(J)-PART</td>
<td>SE-MAODV</td>
<td>SE-MAODV</td>
<td>SE-MAODV</td>
<td>SE-MAODV</td>
<td>SE-MAODV</td>
</tr>
<tr>
<td>GLS</td>
<td>EC-MAODV</td>
<td>EC-MAODV</td>
<td>EC-MAODV</td>
<td>EC-MAODV</td>
<td>EC-MAODV</td>
</tr>
<tr>
<td>FLB</td>
<td>EC-MAODV</td>
<td>EC-MAODV</td>
<td>EC-MAODV</td>
<td>EC-MAODV</td>
<td>EC-MAODV</td>
</tr>
<tr>
<td>GLP</td>
<td>EC-MAODV</td>
<td>EC-MAODV</td>
<td>EC-MAODV</td>
<td>EC-MAODV</td>
<td>EC-MAODV</td>
</tr>
</tbody>
</table>

- Based on Tables VII and VIII, DoS is the only attack that can be confronted by all multicast classification combinations. i.e., there is at least one protocol that classified by all classification dimension (Routing Scheme, Multicast topology, Initialization approach and Maintenance approach) can confront the DoS attack as showed in Table VIII.
- The protocol that confront rushing attack can cover other attacks which related to rushing attack such as blackhole and jellyfish attacks.
- SEAMAN (which is based on symmetric cryptography key, certificate server and HMAC) is the protocol that confront various attacks such as DoS, location disclosure, selfish, and spoofing attacks. In addition, the asymmetric and symmetric cryptography key security techniques are frequently used in securing various multicast operations in almost discussed protocols.
- Selfish is one of the least confronted attack, as selfish attack is an internal attack that can be launched from legitimate nodes which is hard to discover.
REFERENCES


