A Survey on Security Enhanced Multicast Routing Protocols in Mobile Ad Hoc Networks

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

Abstract—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 inherit 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. This paper presents a comprehensive survey on multicast routing protocols along with their security techniques and the types of attacks they can confront. A comparison for the capability of the various secured multicast routing protocols against the identified attacks is also presented.

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

I. INTRODUCTION

A mobile ad-hoc Network (MANET) is a self-organized network of mobile nodes that communicate through wireless links. 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 [1], [2]. 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 via several unicast connections, multicasting minimizes channel capacity consumption, sender and router processing, energy consumption, and communication delay [2], [3].

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 [4] 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 [5].

The objective of this paper is to provide a comprehensive survey on multicast routing protocols for MANETs. The operational concepts of the main multicast routing protocols are first identified and summarized. Then, well-known attacks that represent threats to the security of various multicast operations are summarized and discussed. We then survey some of the key security techniques, and investigate the capability of secured protocols with respect to various attacks.

The rest of the paper is organized as follows. Section II presents classifications for multicast routing protocols. Section III presents brief overview on some of the main multicast routing protocols in the literature. Section IV presents short description for the main types of attacks on MANETs. Section V presents brief details about some techniques for securing the multicast routing protocols discussed in section III. Section VI summarizes the paper.

II. CLASSIFICATION OF MULTICAST ROUTING PROTOCOLS

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

In this paper, we focus only on the IPLM multicasting. To better understand multicasting in this layer, 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.

Figure 1 shows the various classifications of the multicast routing protocols in MANETs. It illustrates the main classification dimensions for multicast routing protocols such as: multicast topology, initialization approach, routing scheme, and maintenance approach. We can conclude from Figure 1 the dependencies between the different dimensions of the multicast routing protocols. For example, shared tree located under tree based approach which locate under multicast topology in the multicast routing protocol design considerations.
Fig. 1. Classification dimensions of multicast routing protocols

A. Multicast Topology

Multicast topology is classified into three approaches namely tree-based, mesh-based, and stateless approach [2], [3]. The three approaches are described as the following:

1) **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. 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 approaches: (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 [3].

2) **Mesh-based approach**, in contrast to a tree-based approach, mesh-based multicast protocols may have multiple paths between any source and receiver pair. In MANET 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 few 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 [3].

B. Routing Initialization Approach

Routing initialization can be classified into three approaches namely source-initiated, receiver-initiated, and hybrid approach [1]. The three approaches are described as the following:

1) **Source-initiated approach**. In this approach, the multicast group performs construction and maintenance tasks are done by the source node. In order to initiate a new multicast group, the source node broadcasts a join query message all over the network and every node that wants to join this multicast group replies with join reply message [1].

2) **Receiver-initiated approach**. In this approach, 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 broadcasts a join query message all over the network and the source node or a core node replies with join reply message with multicast group core route [1].

3) **Hybrid approach**. This approach 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 [1].

C. Routing Scheme

Routing scheme is classified into three approaches namely table-driven, on-demand, and hybrid approach [1], [3]. The three approaches are described as the following:

1) **Proactive**, also called “table-driven”. 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 [3].

2) **Reactive**, also called “on-demand”. 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 [3].

3) **Hybrid** multicast routing protocols, 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 [3].

D. Multicast Maintenance Approaches

Multicast maintenance is classified into two approaches namely Soft-State, and Hard-State approach [1]. The two approaches are described as the following:

1) **Soft-state approach**. In this approach, route maintenance process initiated periodically by flooding the network with control packets to explore other routes between source and receiver. This approach has the advantage of reliability and better packet delivery ratio, but it is much makes overhead over the network as it continuously flood the network with control packets [1].
2) **Hard-state approach.** In this approach, route 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 [1].

### III. Multicast Routing Protocols in MANETS

This section summarizes some of most common multicast routing protocols used in MANETs. Namely MZRP [6], MAODV [7], AMRIS [8], ODMRP [9], MANSI [10], ABMRS [11], PLBM [12]. We present a brief description, key limitation, and security challenges of the described protocols.

Table I presents a comprehensive representation of the multicast routing protocols classification (which only operate on network and application layers) in which it provide a tabular view of routing scheme, initialization of multicast connectivity, multicast topology, and multicast topology maintenance.

<table>
<thead>
<tr>
<th>Protocol Name</th>
<th>Hybrid</th>
<th>Reactive</th>
<th>Proactive</th>
<th>Shared tree</th>
<th>Source tree</th>
<th>Mesh based</th>
<th>Receiver</th>
<th>Source</th>
<th>Agent</th>
<th>Hard state</th>
<th>Soft state</th>
</tr>
</thead>
<tbody>
<tr>
<td>MZRP [6]</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAODV [7]</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AMRIS [8]</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ODMRP [9]</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MANSI [10]</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ABMRS [11]</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PLBM [12]</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### A. Multicast Routing Protocol Based on Zone Routing (MZRP)

MZRP [6] is a source-initiated multicast protocol that combines reactive and proactive routing approaches. When a node has multicast packets to send but no route information is available, it starts to create a forwarding mesh in the entire network. Then, it creates multiple mesh-based routing zones, including source and branch zones, along the route from source node to multicast receiver nodes according to the distribution of source node, receiver nodes and forwarding group nodes in the forwarding mesh.

Zone leaders are selected according to First Declaration Wins (FDW) principle which is responsible for creating and maintaining zones periodically. Inside each zone, a mesh-based multicast routing strategy. Zone size and the number of zones can be decided according to the network size and multicast nodes distribution. Tunneling technique is employed to deliver multicast packets among zones and other sporadic multicast receivers that are not included in any zone in which multicast packets are encapsulated in the unicast packet for transmission. Since control packets flooding is restricted inside multicast zones, multicast overhead will be vastly reduced, and good scalability can be obtained.

### B. Multicast Ad Hoc On-Demand Distance Vector (MAODV)

The MAODV protocol [7] is considered to be an integral part of Ad-hoc On demand Distance Vector Protocol (AODV) [13] which can perform unicasting, broadcasting and multicasting. MAODV is an on-demand tree based protocol, in which nodes those are not members of the group but their position are very critical for forwarding the multicast information. When a node wishes to send a message, it discovers a route and using this route it sends that message. If a node wants to join a multicast group or wants to send a message which has no prior route to that group, then that node sends a Route Request (RREQ) message.

If a member node wishes to terminate its group membership, that node has to ask for the termination to the group. Then its membership will be terminated. Each multicast group has a unique address and a group sequence number. The group member that first constructs the tree is the group leader for that tree, which is responsible for maintaining the group tree by periodically broadcasting Group Hello (GRPH) message. Each node has three tables namely unicast route table, multicast route table, and group leader table. Unicast route table has an address of the next hop to which the message is to be forwarded. Multicast route table has the address of the next hops for the tree structure of the each multicast group. The Group leader table records the current multicast group addresses with its group leader address and the next hop address towards that group leader receives a periodic GRPH message.

### C. Ad Hoc Multicast Routing Protocol Utilizing Increasing ID Numbers (AMRIS)

AMRIS [8] is an on-demand protocol which constructs a shared delivery tree to support multiple senders and receivers within a multicast session. The key idea that differentiates AMRIS from other multicast routing protocols is that each participant in the multicast session has a session-specific multicast session member id (msm-id). The msm-id provides each node with an indication of its “logical height” in the multicast delivery tree. Each node except the root must have one parent that has a logical height (msm-id) that is smaller than it.

The ordering between id-numbers is used to direct the multicast flow, and the sparseness among them used for quick
connectivity repair. A multicast delivery tree rooted at a special
node called (Sid) joins up the nodes participating in the
multicast session. The relationship between the id-numbers
(the nodes that own them) and Sid is that the id-numbers
increase in numerical value as they radiate from Sid in the
delivery tree. These id-numbers help the nodes dynamically
leave and join a session, as well as adapt rapidly to changes
in link connectivity.

D. On-Demand Multicast Routing Protocol (ODMRP)

ODMRP [9] is a mesh-based, multicast protocol that pro-
vides richer connectivity among multicast members. By build-
ing a mesh and supplying multiple routes, multicast packets
can be delivered to destinations in the face of node movements
and topology changes. In addition, the drawbacks of multicast
trees in mobile wireless networks (e.g., traffic concentration,
frequent tree reconfiguration, non-shortest path in a shared
tree, etc.) are avoided. To establish a mesh for each multicast
group, ODMRP uses the concept of forwarding group. The
forwarding group is a set of nodes responsible for forward-
ing multicast data on shortest paths between any member
pairs. ODMRP also applies on-demand routing techniques
to avoid channel overhead and improve scalability. A soft
state approach is taken to maintain multicast group members.
No explicit control message is required to leave the group.
The reduction of channel/storage overhead and the richer
connectivity make ODMRP more attractive in mobile wireless
networks.

E. Multicast for Ad Hoc Networks with Swarm Intelligence
(MANSI)

Swarm intelligence [10] refers to complex behaviors that
arise from very simple individual behaviors and interactions,
which is often observed in nature, especially among social
insects such as ants. Although each individual has little intel-
ligence and simply follows basic rules using local information
obtained from the environment, such as ant’s pheromone trail
laying and following behavior, globally optimized behaviors,
such as finding a shortest path, emerge when they work
collectively as a group. MANSI utilizes small control packets
equivalent to ants in the physical world. These packets, trav-
eling like biological ants, deposit control information at nodes
they visit, similar to the way ants laying pheromone trails. This
information, in turn, affects the behavior of other ant packets.
With this form of indirect communication, the deployment of
ant-like packets resembles an adaptive distributed control sys-
tem that evolves itself to a more efficient state, accommodating
the current condition of the environment.

For each multicast group, MANSI determines a set of
intermediate nodes, forming a forwarding set, that connect
all the group members together and are shared among all
the group senders. By adopting a core-based approach, the
forwarding set will evolve, by means of swarm intelligence,
over time into states that yield lower cost, which is expressed
in terms of total cost of all the nodes in the forwarding set.
This evolving, including exploring and learning, mechanism
differentiates MANSI from other existing ad hoc multicast
routing protocols. Since a node’s cost is abstract and may be
defined to represent different metrics, MANSI can be applied
to many variations of multicast routing problems for ad hoc
networks.

F. Agent-Based Multicast Routing Scheme (ABMRS)

types of agents are used in the scheme: route manager static
agent, network initiation mobile agent, network management
static agent, multicast initiation mobile agent, and multicast
management static agent. The scheme operates in the follow-
ing steps: (1) To identify reliable nodes, (2) To connect reliable
nodes through intermediate nodes, (3) To construct a backbone
for multicasting using reliable nodes and intermediate nodes,
(4) To join multicast group members to the backbone, (5) To
perform backbone and group members management in case of
mobility.

The protocol assumes availability of an agent platform at
all the mobile nodes. However, in case of agent platform un-
availability, traditional message exchange mechanisms can be
used for agent communication. The agent based architectures
provide flexible, adaptable and asynchronous mechanisms for
distributed network management, and also facilitate software
reuse and maintenance. The work can be extended to construct
multiple multicast trees to provide fault redundancy. There
are certain overheads associated with the agent based scheme
such as maintaining an agency database, maintaining multicast
route information, creation of an agent platform and agent
communication.

G. Preferred Link-Based Multicast Protocol (PLBM)

PLBM [12] is a tree-based receiver-initiated protocol.
PLBM is a routing protocol with efficient flooding mech-
anisms. The main objective of PLBM is to find a single
preferred link from the source to the destination node. In
PLBM each node owns a Neighbor List (NL) which is updated
with the neighbor beacons. This subset of nodes is also stored
in a Preferred List (PL). Now when a route-request message is
send out, only the nodes listed in the PL forward the message.
Also Neighbor’s Neighbor Table (NNT) is used to maintain
information of the neighbors and their neighbors. PLBM
consists of 3 phases: route establishment, route selection and
route maintenance.

PLBM has two different algorithms: (a) neighbor degree-
based preferred link algorithm, this algorithm selects the path
with the degree of a node which means the number of nodes.
Nodes with a higher degree are preferred to node with a lower
degree. All the nodes that have a higher degree have more
nodes listed in their NNT and so fewer nodes can be selected.
(b) Weight Based Preferred Link (WBPL) algorithm, each
node has its own weight. This weight is used to find stable links thought the network. WBPL considers the stability of the link between the nodes.

IV. MAIN ROUTING ATTACKS IN MANETS

The security issue of MANETs in group communications is even more challenging because of the involvement of multiple senders and multiple receivers. Although several types of security attacks in MANETs have been studied in literature, the focus of earlier research is on unicast communication. In this section, we summarize the most common types of attacks on multicast routing protocols in MANET.

- **Rushing Attack** [14]: 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** [15]: A blackhole attacker first needs to invade into 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** [15]: 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** [15]: 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** [16]: 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** [17]: 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** [15]: 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** [18]: 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.

V. SECURITY TECHNIQUES FOR MULTICAST ROUTING PROTOCOLS IN MANETS

This section summarize some of most common security techniques for routing protocols in MANETs. These security techniques not designed specially for multicast routing protocols, however it can be extended to cover the attacks that confront the multicast routing protocols, as well as the unicast routing protocols.

Table II summarizes the main features of the described security techniques and its performance aspects, as well as the secured multicast protocols which extend. Table II includes the main objectives, the applied basic security mechanisms, specific design considerations, performance aspects cover adaptation to topology changes, scalability with the number of nodes, packet overhead and processing overhead of security techniques. The intention of this performance classifications is rather a high level qualitative estimation of secure routing approaches than a precise quantitative performance evaluation.

For each security technique, we summarize the main objectives and security mechanisms. Then, we describe how each approach works. The security techniques described in this section are: ARAN [19], SRP [21], SEAD [24], ARIADNE [25] and SAODV [26].

A. Authenticated Routing for Ad hoc Networks (ARAN)

ARAN [19] is on-demand protocol similar to MAODV [7], but it provides secure routing for the managed open environments. ARAN provides authentication and non-repudiation services using cryptographic certificates that guarantees end-to-end authentication. In doing so, ARAN limits or prevents attacks that can afflict other insecure protocols.
## SECURITY ROUTING TECHNIQUES FEATURES

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ARAN [19]</td>
<td>MAODV [7]</td>
<td>Asymmetric cryptography key and certificate server [20]</td>
<td>Based on AODV [13], and designed to secure reactive routing protocols</td>
<td>Good adaptation</td>
<td>Average scalability</td>
<td>Average overhead</td>
<td>High processing</td>
<td></td>
</tr>
<tr>
<td>ARIADNE [25]</td>
<td>AMRIS [8]</td>
<td>Symmetric cryptography key [22] and hash chain function [23]</td>
<td>Based on the basic operations of DSR protocol</td>
<td>Average adaptation</td>
<td>Average scalability</td>
<td>Low overhead</td>
<td>Average overhead</td>
<td></td>
</tr>
</tbody>
</table>

ARAN is a simple protocol that does not require significant additional work from nodes within the group. ARAN is as effective as MAODV in discovering and maintaining routes. The cost of ARAN is larger routing packets, which result in a higher overall routing load, and higher latency in route discovery because of the cryptographic computation that must occur. ARAN uses public-key cryptographic mechanisms to defeat all identified attacks. ARAN can secure routing in environments where nodes are authorized to participate but untrusted to cooperate, as well as environments where participants do not need to be authorized to participate.

### B. Secure Routing Protocol (SRP)

SRP [21] is a lightweight security for Dynamic Source Routing (DSR), which can be used with DSR to design SRP as an extension header that is attached to Route Request (RREQ) and Route Reply (RREP) packets. SRP doesn’t attempt to secure RERR packets but instead delegates the route maintenance function to the secure route maintenance portion of the secure message transmission protocol.

Message Authentication Code (MAC) plays an important role in SRP. The source node sets up the route discovery and constructs a route request packet by a pair of identifiers: a query sequence number and a random query identifier. The source and destination and the unique query identifiers are the input for the calculation of the MAC. When receiving a route request, if it is a fresh one, the intermediate nodes add its IP address to the route request. Then it relay the request, so that when query packets arrive at the destination, only a limited amount of state information are needed to be maintained regarding the relayed queries. Thus previously seen route requests are discarded at the destination.

### C. Secure Efficient Ad hoc Distance Vector routing (SEAD) protocol

SEAD [24] is designed with the objective to protect against multiple uncoordinated attackers creating incorrect routing state in any other node. In order to be deployed in an environment with low computational power and to guard against DoS attacks in which an attacker tries to make other nodes consume excessive bandwidth or processing time, it only uses efficient one-way hash functions instead of asymmetric operations. The design was based in Destination-Sequence Distance-Vector (DSDV) protocol, but the main ideas can be applied in other distance vector protocols.

SEAD do not use an average weighted settling time in sending triggered updates. To reduce the number of redundant triggered updates, each node in DSDV tracks, for each destination, the average time between: when the node receives the first update for some new sequence number for that destination, and when it receives the best update for that sequence number for it. When deciding to send a triggered update, each DSDV node delays any triggered update for a destination for this average weighted settling time, in the hope of only needing to send one triggered update, with the best metric, for that sequence number.

### D. ARIADNE

ARIADNE [25] prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents a large number of types of denial-of-service attacks. In addition, ARIADNE is efficient, using only highly efficient symmetric cryptographic primitives. The main objective of ARIADNE is to provide authentication and integrity of Dynamic Source Routing (DSR) signaling messages, i.e., routing discovery and route maintenance. With DSR, a Route Request (RREQ) carries the node list for the source route. In order to provide a reliable route discovery ARIADNE verifies authenticity and integrity of a RREQ making it infeasible to remove nodes from the list and to ensure senders’ authenticity.
E. Secure Ad-hoc On-demand Distance Vector (SAODV) Protocol

SAODV [26] is a proposal for security extensions to the Ad-hoc On-demand Distance Vector (AODV) protocol [13]. The proposed extensions utilize digital signatures and hash chains in order to secure AODV packets. In particular, cryptographic signatures are used for authenticating the non-mutable fields of the messages, while a new one-way hash chain is created for every route discovery process to secure the hop-count field, which is the only mutable field of an AODV message. Since the protocol uses asymmetric cryptography for digital signatures it requires the existence of a key management mechanism that enables a node to acquire and verify the public key of other nodes that participate in the ad hoc network.

VI. 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. 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.

This paper presents a comprehensive survey on multicast routing protocols. The capability of multicast protocols along with their security techniques are summarized against various network attacks. Table III presents a comparison between security techniques described in Section V and the well-known types of attacks described in Section IV. The table can be used to identify attacks that are addressed in various multicast routing protocols. Moreover, the table highlights which attacks are covered by each security technique and which attacks are not fully covered yet.

**REFERENCES**