Secure Multicast Routing Algorithm for Wireless Mesh Networks

Rakesh Matam¹ and Somanath Tripathy²

¹Indian Institute of Information Technology, Guwahati, Assam 781001, India
²Indian Institute of Technology Patna, Patna, Bihar 800013, India

Correspondence should be addressed to Rakesh Matam; matamrakesh@gmail.com

Received 5 November 2015; Revised 10 March 2016; Accepted 15 March 2016

Copyright © 2016 R. Matam and S. Tripathy. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Multicast is an indispensable communication technique in wireless mesh network (WMN). Many applications in WMN including multicast TV, audio and video conferencing, and multiplayer social gaming use multicast transmission. On the other hand, security in multicast transmissions is crucial, without which the network services are significantly disrupted. Existing secure routing protocols that address different active attacks are still vulnerable due to subtle nature of flaws in protocol design. Moreover, existing secure routing protocols assume that adversarial nodes cannot share an out-of-band communication channel which rules out the possibility of wormhole attack. In this paper, we propose SEMRAW (Secure Multicast Routing Algorithm for Wireless mesh network) that is resistant against all known active threats including wormhole attack. SEMRAW employs digital signatures to prevent a malicious node from gaining illegitimate access to the message contents. Security of SEMRAW is evaluated using the simulation paradigm approach.

1. Introduction

Wireless mesh networks have emerged as a popular technology to provide wireless Internet access anywhere anytime [1]. Recent popular applications of WMN include multicast TV, audio and video conferencing, and multiplayer social gaming. These multimedia streaming applications rely on multicast transmissions for transportation of content, as it is an efficient way of transmitting same data stream to several clients simultaneously [2]. Multicast data streams are characterized by their requirement of high bandwidth and low latency [3]. Therefore, majority of the existing works mainly focus on optimizing these requirements. At the same time, other requirements such as security are implicitly assumed. However, it has been already shown that failing to address security issues of a routing protocol for WMN can severely disrupt network services and significantly affect performance [4].

A multicast routing protocol is vulnerable to several active attacks. The nature of these attacks is similar in comparison to attacks launched against a unicast routing protocol. However, the impact of an attack in multicast environment is much higher compared to its unicast counterpart, as a single attacker can affect transmissions to multiple destinations at the same time. Therefore, addressing security attacks in multicast environment is considered to be more crucial. Very few works exist that specifically address the security aspects of a multicast routing protocol. The reason behind this can be attributed to the obvious similarity between unicast and multicast routing protocols and the attacks launched against them. This facilitates easy adaptation of unicast security solutions to multicast environment.

Security techniques employed by unicast routing protocols like secure on-demand distance vector protocol (SAODV) [5], authenticated routing in ad hoc networks (ARAN), and [6] security aware routing (SAR) [7] are based on AODV [8]. These security frameworks can be adapted by multicast routing protocols like MAODV [9] and on-demand multicast routing protocol (ODMRP) [10]. On the other hand, Ariadne [11] and secure routing protocol (SRP) [12] are based on dynamic source routing (DSR) [13] and therefore can be adapted by ad hoc multicast routing protocol (AMRIS) [14]. But vulnerabilities still exist mainly due to the subtle nature of flaws in these protocols [15]. Moreover, the adversary model employed by these secure routing protocols restricts colluding malicious nodes from sharing a hidden/out-of-band channel which rules out wormhole...
attack. So these drawbacks would be inherent to adapted secure multicast routing protocols. Alternative works like Byzantine-resilient multicast routing BMSR [16] and Secure-ODMRP [17] are multicast routing specific security protocols that rely on the transmission behavior of mesh routers to detect and avoid malicious nodes while establishing multicast routes. Therefore, there is a call for secure multicast routing schemes that can defend against all known active attacks.

In this paper, we present a secure multicast routing algorithm SEMRAW (SEcure Multicast Routing Algorithm for Wireless mesh network), the secure version of our previous work enhanced multicast routing algorithm for WMN EMRAW [18], SEMRAW thus preserves the performance merits of EMRAW, by selecting paths that incur fewer number of transmissions and establishing a bandwidth minimal multicast tree. It scales well compared to other multicast algorithms, specifically in scenarios where multicast receivers are sparsely distributed. SEMRAW employs an integrated security approach to address different active security threats even relaxing the restrictions of active-n-m adversary model [19]. The security of the proposed protocol is formally evaluated using simulation paradigm approach [20, 21].

The rest of the paper is organized as follows. Section 2 presents related work. Section 3 presents the network and adversarial model and basic definitions of security used to evaluate the proposed protocol. Section 4 presents the proposed algorithm secure EMRAW. The security proof of the proposed algorithm is presented in Section 5. Section 6 presents the simulation results of SEMRAW. In Section 7, we present a brief discussion on the robustness of SEMRAW and finally Section 8 provides the concluding remarks.

2. Related Work

Even though the security frameworks of existing unicast secure routing protocols like SAODV [5], ARAN [6], SAR [7], Ariadne [11], and SRP [12] can be adapted by multicast routing protocols like M-AODV [9], ODMRP [10], and AMRIS [14], they are still vulnerable to some security threats. The formal analysis of these protocols has uncovered subtle flaws that are otherwise difficult to identify [15, 22–26]. Moreover, the security of these protocols is evaluated against an active-n-m adversary model that prohibits adversaries from sharing an out-of-band channel which rules out wormhole attacks [23].

Multicast specific secure routing protocols like BMSR [16] and SODMRP [17] focus on addressing Byzantine attacks like flood rushing, packet dropping, and wormhole attacks. These are essentially detection based schemes that rely on the transmission behavior of mesh routers to detect and avoid malicious nodes while establishing routes. BMSR is a Byzantine-resilient multicast protocol that detects Byzantine attacks (attacks launched by nodes that are legitimate part of the network) based on the packet dropping behavior of mesh routers. Specifically, nodes in BSMR determine the reliability of their direct links by comparing the observed data rate with the data rate advertised by the source node. If the observed data rate falls below the rate indicated by the source node by more than a threshold, the neighboring node sharing a direct link with the adversarial node updates its weight list and initiates a new route discovery process by including the weight lists of the links in the route requests. The major limitation of BMSR is its reliance on static detection threshold, which is independent of the channel quality and medium access collisions. Similarly, SODMRP is a secure high-throughput multicast protocol based on ODMRP and link layer metric, SPP (success probability product) [27]. SODMRP addresses packet dropping attacks by detecting the discrepancies between expected packet delivery ratio (ePDR) and perceived packet delivery ratio (pPDR). A node estimates the ePDR of a route from SPP of that route and a node determines the pPDR for a route by measuring the rate at which it receives data packets from its upstream node on that route. If ePDR-pPDR for a route becomes larger than a detection threshold, then nodes suspect that the route is under attack because the route failed to deliver data at a rate consistent with its claimed quality.

Besides these, other works like HASM [28], MeCA [29], and the secure multicast protocols proposed in [30–32] focus on key generation, key management, and secure group communication techniques to protect against outside attacks. Hierarchical agent based secure multicast (HASM) is one such agent based secure multicast algorithm for securing mobile multicast in WMNs. It aims at minimizing the overall network communication cost incurred by multicast packet delivery, security key management, group membership maintenance, and mobility management. HASM dynamically maintains a group of multicast agents running on mesh routers for integrated mobility and multicast service management and maintains a hierarchical multicast structure for efficient multicast packet delivery.

Mesh certification authority (MeCA), presented in [29], addresses the problem of authentication and key management without a trusted third party in wireless mesh networks. It relies on the self-configuring and self-organizing characteristics of WMN to distribute the functions of a certification authority over several mesh routers. Key functionalities like secret sharing and key distribution are based on threshold cryptography, which minimizes the possibility of secret disclosure even when some shareholders are compromised by adversaries. MeCA adopts the multicast tree building approach presented in [33] to reduce the operation overhead.

Similar to MeCA, the secure multicast framework proposed in [31] is decentralized and exploits the self-healing characteristics of wireless mesh network. It is based on the multihop proxy encryption scheme that is first employed in [34], to secure group communications. The source that initiates the communication generates the topology aware key encryption keys (KEK) after the initialization and the key path construction. The session key, used as the traffic encryption key (TEK), is distributed by a new multihop proxy encryption with the KEKs along the key path. Subprotocols like rekeying and self-healing are employed to handle new joins and router failures.

Reference [35] presents a certificateless architecture for multicast wireless mesh network. It uses certificateless proxy reencryption mechanism. It relies on a transformation technique that reduces cipher texts from $k \cdot n$ size to $k + n$, where
$k$ denotes the length of the best route from the source to the target multicast users and $n$ denotes the number of valid receivers in the group.

A key point to note is that none of the existing schemes single handedly address all of the active security attacks on multicast routing protocols in WMN. The existing security frameworks for unicast routing protocols cannot be applied for multicast environment due to their vulnerabilities and limitations. Multicast routing specific protocols like BSMR [16] and SODMRP [17] employ different detection mechanisms to successfully address malicious packet dropping attacks. Other works like HASM [28] and MeCA [29] address issues like secure key distribution, key management, and secure group communication in multicast environment. In this paper, we present SEMRAW that employs integrated security framework to address all active attacks on multicast routing protocols in WMN.

3. System Model

In this section, we present the network and adversarial model. We also briefly present the system model used to evaluate the security of the proposed protocol. The same system model has been employed in our earlier work [21] to prove security of another protocol. The definitions of system correctness and the security are similar to those defined in [21].

3.1. Network Model. We consider a typical wireless mesh network (WMN) architecture, where a set of MRs that are uniformly distributed, form the backbone of WMN. Few of these mesh routers (MRs) designated as gateways can be connected to the Internet. Mesh clients (MCs) are typical wireless clients connected to specific MRs with access point functionality. We model the backbone of the WMN as a undirected labelled graph $G(V,E)$, where $V$ is the set of vertices and $E$ is the set of edges. Each MR represents a node, and there is an edge between two vertices if and only if there is a communication link between the corresponding nodes. The communication links between nodes are assumed to be bidirectional. Each link is assigned a cost by a node connected to it with the help of a cost function $C_{\text{Link}} : E \to \mathbb{R}$, to represent the routing metric.

3.2. Security Model

3.2.1. Security Assumptions. We assume that all network nodes obtain a valid certificate signed by the certification authority (CA) that is later used for authentication. Nodes use authenticated identifiers for secure peer link establishment and construction of a multicast tree. SEMRAW relies on two-hop neighborhood information for establishing routes; therefore, during neighbor discovery, a node authenticates itself with all the nodes in its two-hop range by presenting a valid certificate and thereby validating its neighborhood. The set of node-identifiers are denoted by $L$ and we label each vertex $v$ of $V$ in $G$ with the identifiers used by the node corresponding to $v$. Each nonmalicious node in the network uses a single identifier that is unique in the network, whereas malicious nodes may use multiple identifiers of the compromised ones. The set of malicious nodes and their identifiers is represented by $V^*$ and $L^*$, respectively. The assignment of identifiers to the nodes is represented by a labelling function $\Phi : V \to 2^L$, which returns the set of labels assigned to each vertex $v$ in $G$. If $v$ corresponds to a noncompromised node, then $\Phi(v)$ is a singleton and $\Phi(v) \notin \Phi(v')$ holds for any other vertex $v'$. Here, the configuration conf is represented as a 4-tuple $(G(V,E), V^*, \Phi, C_{\text{Link}})$. It consists of a network graph, the set of compromised nodes, the labelling function, and cost function.

3.2.2. Adversarial Model. We consider a class IX attacker model as presented in [19]. A class IX adversary has all the capabilities of an active-n-m attacker and an additional capability that allows colluded malicious nodes to establish an out-of-band communication link between themselves to relay messages. In an active-n-m adversarial model $n$ signifies the number of compromised MRs that hold keying material, and $m$ is the total number of attacker nodes in the network. Usually, attacker nodes in the active-n-m attacker model have restricted capabilities that prevent them from sharing information through out-of-band channels, which rules out wormhole attacks. An attacker in a class IX attacker model can launch various kinds of active attacks involving modification, metric manipulation, and fabrication of routing messages. An adversary can also launch a wormhole attack by colluding with other malicious nodes. The major motivation of the attacker is to corrupt the routing protocol to launch various kinds of active denial of service (DoS) attacks, to disrupt network services.

3.3. System State. State of the system $Q$ can be represented by the set of verified routing entries of tables of all uncompromised nodes. A routing entry in $v$’s routing table can be represented as a five-tuple field $(v, l_{\text{tar}}, l_{\text{nxt}}^1, l_{\text{nxt}}^2, C)$ in $Q$ with identifier $l_{\text{tar}}$ as target and $l_{\text{nxt}}^1$ as the one-hop and $l_{\text{nxt}}^2$ as the two-hop identifier with routing metric $C$. Thus, the system state $Q \subset (V \setminus V^*)$ is a collection of such tuples. A system is said to be in a correct state if all the verified routing entries of uncompromised nodes are correct; that is, if $v$ has a verified routing entry for target $l_{\text{tar}}$ with one-hop $l_{\text{nxt}}^1$ and two-hop $l_{\text{nxt}}^2$, with cost $C$, then actually there exists a route that starts at node $v$ and ends at node $l_{\text{tar}}$ and the path through $l_{\text{nxt}}^1$ and $l_{\text{nxt}}^2$ is comprised of edges only belonging to $E$ and with the metric value $C$.

Definition 1 (correct state). The state $Q$ of a system is said to be correct if for every $(v, l_{\text{tar}}, l_{\text{nxt}}^1, l_{\text{nxt}}^2, C) \in Q$, there exists a sequence $v_1, v_2, \ldots, v_p$ of vertices in $V$ such that $(v_i, v_{i+1}) \in E$ (for all $1 \leq i < p$), and

(i) $v_1 = v$,
(ii) $l_{\text{tar}} \in \ell(v_p)$,
(iii) $l_{\text{nxt}}^1 \in \ell(v_2)$,
(iv) $l_{\text{nxt}}^2 \in \ell(v_3)$,
model can be “almost perfectly” simulated by an ideal-world adversary in the ideal-world model. That is, no ideal-world adversary exists that can cause the ideal-world system to go into an incorrect state, and it follows that no real-world adversary can exist that can cause the real-world model to move into an incorrect state with nonnegligible probability because if such an adversary exists, then no ideal-world adversary can simulate it "almost perfectly.”

4. SEMRAW: The Proposed Secure Multicast Routing Algorithm

The proposed secure multicast routing algorithm for WMN is based on our multicast routing protocol EMRAW [18]. SEMRAW employs an integrated security scheme to prevent all the active attacks on a multicast routing protocol in wireless mesh networks. SEMRAW requires every node to maintain secure neighborhood relations with all the nodes in its two-hop range. To prevent malicious nodes from manipulating the accumulated metric, the multicast routing messages are protected with the help of signatures. SEMRAW mainly prevents nodes from modifying the metric field appended by previous nodes in the network. Multicast tree formation in SEMRAW is accomplished by a broadcast tree establishment message from a source node that is replied back by the set of receivers.

SEMRAW uses signatures to provide authentication and message-integrity to the tree establishment process. Therefore, it uses the services of a trusted certificate server, whose public key is known to all valid nodes. Each node maintains a list of public keys of all the nodes in its one-hop and two-hop neighborhood. The public and private keys of a node are represented by $K^C_A$ and $K^S_A$, respectively. It also employs a wormhole detection mechanism presented in [36] to distinguish real links from links traversing a wormhole. The proposed SEMRAW operates in following 3 phases.

4.1. Request Phase. The request phase is initiated by the source $S$ (source node in the sample network shown in Figure 1), whenever it needs to form a multicast group or establish/update routes with the members of multicast group. In either case, $S$ needs to establish multicast routes with the set of group members (receivers). $S$ initiates the request phase by flooding a Join Request (JRQ), advertising the multicast group. The contents of Join Request include Multicast Address (MA), Multicast Request ID (MID), Sequence Number (SN), Source Address (SA), Transmitter Address (TA), Hop Count (HC), Metric Value, and Time-to-Live (TTL). The Join Request identity (JRQ-ID) uniquely identifies a Join Request. On receiving a nonduplicate Join Request (JRQ), intermediate nodes rebroadcast it after creating a routing entry for the received Join Request. Meanwhile, multicast receivers that receive the Join Request respond to it with a Join Reply, initiating the Reply phase:

$$S \rightarrow \ast : \{JRQ, 2HA, 3HA, 4HA\} K^S_2 [M_B, HC, S, SQ] K^C_2. \quad (1)$$

JRQ represents the contents of the JRQ element. The 2HA represents the address of previous hop from which
the current transmitting node received the JRQ. It is not applicable to the source node transmitting the JRQ. 3HA and 4HA represent the 3rd and 4th hop address that the JRQ has traversed. 3HA and 4HA enable SEMRAW to distinguish real links from out-of-band links. SEMRAW allows nodes to monitor the two-hop subpath on a received Join Request and identify a JRQ that traverses an out-of-band link like a wormhole. A JRQ that traverses an out-of-band link would not satisfy the necessary wormhole-free path criterion [36], which can be detected at the neighbors of a wormhole node and is quarantined. A path is said to be free from wormhole links if and only if for each subpath of length 2R there exists an alternate subpath of maximum length 4R, where R is the transmission range of a node. The probability of finding alternate paths between nodes separated by a distance $d$ ($R < d < 2R$) (in a network where nodes are uniformly distributed) is high. The JRQ element is further extended to include an authenticated metric field that contains the metric, hop count, and source sequence number ($S, S_{SQ}$).

Nodes $I_1$, $I_2$, $I_3$ that receive the JRQ from $S$ verify its authenticity by validating the signatures. Once verified, a node creates a multicast routing entry towards the source. All routing entries in SEMRAW are by default considered to be in transient state. They are elevated to stable state only after a JRQ is verified to be wormhole-free.

An intermediate node $I_j$ begins the wormhole verification process by checking for an existing transient routing entry corresponding to the MID and sequence number received in JRQ. Multiple transient routing entries may exist for the same MID that are received through a unique two-hop node. Node $I_j$ then compares the two-hop address present in JRQ with the two-hop addresses of a set of existing routing entries represented by $JRQ_o$. If it matches with any of the existing routing entries $JRQ_o$, it is updated with JRQ provided that it offers better metric. In case of no matching address, node $I_j$ further compares the three-hop and four-hop addresses present in JRQ with the two-hop addresses of routing entries represented by $JRQ_o$ or vice versa (provided the 2HA of JRQ does not match with TA address of $JRQ_o$ or vice versa). If any one of the two addresses match (two-hop address in JRQ with three/four-hop addresses of $JRQ_o$ or vice versa), an optimal of the two JRQs ($JRQ_o$ or JRQ) is selected and state of the routing entry is set to stable. If none of the comparisons match, a new transient routing entry is created for the corresponding JRQ-ID. This matching of addresses is carried out to select an optimal wormhole-free path.

Before rebroadcasting the JRQ, nodes $I_1$, $I_2$, and $I_3$ set the 2HA field with address of $S$, respectively. Nodes $I_1$, $I_2$, and $I_3$ also compute the cumulative metrics $M_{I_1}$, $M_{I_2}$, and $M_{I_3}$ (from $I_1 \rightarrow S$, $I_2 \rightarrow S$, and $I_3 \rightarrow S$), respectively. The metric field along with the source sequence number ($S, S_{SQ}$) is independently signed and appended to the JRQ. The source sequence number in the appended metric field ensures the freshness of the JRQ. The metric originally appended by $S$ is kept intact:

$$I_1 \rightarrow * : \{JRQ, S, 3HA, 4HA\} K'_S \{M_S, HC, S_{SQ}\} K'_S \{M_{I_1}, HC, S_{SQ}\} K'_{I_1}.$$  \hspace{1cm} (2)

Similarly, $I_4$ and $I_5$ broadcast the received JRQ after acting on it accordingly. $I_4$ (also $I_5$ and $I_6$) that receives the JRQ from $I_1$ (also $I_2$ from $I_5$ and $I_6$ from $I_3$) verifies the authenticity of the JRQ and the authenticated metric field appended by $S$ and $I_j$. On verifying the authenticity, $I_4$ acts accordingly on the JRQ by computing the cumulative metric, incrementing the hop count and updating the 2HA and 3HA fields. The authenticated metric field appended by $S$ is discarded to include the current cumulative metric $M_{I_4}$, signed and appended by $I_4$. This process is repeated by each intermediate node until the JRQ reaches the set of receivers. The JRQ broadcasted by $I_4$ is given by

$$I_1 \rightarrow * : \{JRQ, S, I_4, 4HA\} K'_{I_4} \{M_{I_4}, HC, S_{SQ}\} K'_{I_4} \{M_{I_4}, HC, S_{SQ}\} K'_{I_4}.$$  \hspace{1cm} (3)

4.2. Reply Phase. The reply phase can be considered as request phase concurrently initiated by the set of receivers to optimize the multicast tree. Reply phase begins when a receiver(s) responds to a Join Request by broadcasting a Join
Journal of Computer Networks and Communications

4.3. Route Commit Phase. The route commit phase is carried out by the source S after receiving Join Replies from the set of receivers. The source selects a route based on the received Join Replies that minimizes overall transmission count in the network. The route is committed by the source by explicitly sending a commit message (RCOM). The contents of route commit message include Multicast Address (MA), Sequence Number (SN), Source Address (SA), Transmitter Address (TA), and Selected Next-Hop address. SNH is the address of selected next-hop that allows a node to realize the path to be followed to a receiver. The route commit message transmitted by source S in the example network is given by

\[ S \rightarrow I_2 : \{RCOM \} K_S^\nu. \]  

Each intermediate propagates the received route commit message through the selected next-hop node towards the receiver(s), after appropriately signing it. Intermediate nodes that act as forwarders for multiple receivers (like I_2 in the current example), propagate an individually signed route commit message through the respective selected forwarder.

5. Security Proof

Theorem 3. The proposed SEMRAW is statistically secure if the signature scheme is secure against chosen message attacks.

Proof. In order to prove the security of SEMRAW, let us construct an appropriate ideal-world adversary A' as discussed in Section 3 for any real-world adversary A. Next, initialize both the systems with the same configuration conf and the same random input r. The proposed algorithm is said to be secure if the output (Out_{ideal, A'}) of the ideal-world model for ideal-world adversary A' is statistically indistinguishable from the output of a real-world model (Out_{real, conf, A}) for any adversary A. In this case, sys_{conf, A} and sys_{ideal, conf, A} are identical implying that, in each step, the state of the corresponding machines and the content of the corresponding tapes are the same. On the other hand, if an incorrect state is encountered, the output configurations of both the models do not match as the ideal-world model outputs a special symbol ($). A system moves into an incorrect state when a routing entry of a noncompromised node \( v \) is incorrect. Node \( v \) sets a routing entry \( (l_{tar}^1 l_{nxt}^1 l_{nxt}^2 C) \) for a target \( l_{tar} \) only if it has received a signed JRQ message which has been traversed through \( l_{nxt}^2 \) and \( l_{nxt}^1 \) with metric equal to \( C \) and the edge \( (l_{nxt}^2 l_{nxt}^1) \in E. \)
Now, the node $v$ shares one-hop and two-hop neighborhood relations with $l_{\text{nxt}}^1$ and $l_{\text{nxt}}^2$. The routing entry can be made incorrect forcing one of the following cases to occur.

**Case 1.** There is no route from $v$ to a node that uses the label $l_{\text{nxt}}$, but attacker forces $l_{\text{tar}}$ to accept the corresponding message.

**Case 2.** There are routes from $v$ to a node that uses the label $l_{\text{tar}}$ going through the one-hop and two-hop neighbors $l_{\text{nxt}}^1$ and $l_{\text{nxt}}^2$ of $v$. But the link between $(l_{\text{nxt}}^1, l_{\text{nxt}}^2) \notin E$. That is, the link is not present in the set of valid edges.

**Case 3.** There are routes from $v$ to a node that uses the label $l_{\text{tar}}$, but the sequence number received in the message through $(l_{\text{nxt}}^1$ and $l_{\text{nxt}}^2$ of $v$) is higher than the original source sequence number.

**Case 4.** There are routes from $v$ to a node that uses the label $l_{\text{tar}}$ going through $l_{\text{nxt}}^1$ and $l_{\text{nxt}}^2$ of $v$. But attacker changes the metric values with cost lower/higher than the actual cost $C$.

To succeed in Case 1, an attacker needs to generate a fabricated JRQ/JRP message that contains the JRQ element and the signed metric fields of the $PrvHopNode$ (through which the JRQ has traversed) and own signed metric field.

In Case 2, to forge a genuine node $v$ into accepting an out-of-band link as a routing entry, it must have also received a Join Request through an alternate path connecting the two-hop node $l_{\text{nxt}}^2$ within a maximum of 4-hops, provided $l_{\text{nxt}}^2$ of newly arrived JRQ does not match with transmitter address of existing Join Request or vice versa. But it has been already proven that finding such an alternate path is negligible in [36]. Therefore, the only way to accept such an incorrect routing entry is by fabricating an alternate Join Request traversing a nonexisting alternate subpath.

In Case 3, for a genuine node $v$ to accept an incorrect routing entry with higher sequence number, the attacker must modify the contents of a JRQ/JRP message such that it has traversed through $l_{\text{nxt}}^1$ and $l_{\text{nxt}}^2$. To perform this, the signature mechanism needs to be forged. Alternatively, if the attacker uses the label ($l'$) of other malicious nodes, node $v$ does not accept such a message since a message traversing $l'$ and $l_{\text{nxt}}^1$ fails in Case 2.

In Case 4, an attacker needs to modify the metric field appended by a $PrvHopNode$ in JRQ/JRP message to force the genuine node $v$ in accepting a route whose metric value is lower/higher than the actual cost $C$. Let $C'$ be the minimum of the costs of routes in $R$. If the signatures of $l_{\text{nxt}}^1$ and $l_{\text{nxt}}^2$ have not been forged, the JRQ must have taken one of the routes in $R$. However, since the metric $C$ is independently signed, the value signed by $l_{\text{nxt}}^2$ cannot be acted upon by $l_{\text{nxt}}^1$ without forging the signature of $l_{\text{nxt}}^2$. Therefore, for $C'$ to be selected over $C$, either $C'$ has to be forged or $C'$ is in fact the best of all the available metric values, which is not the case as $C$ has been selected over $C'$.

Thus the ideal-world model enters into an incorrect state, only if the signature mechanism is forgeable. Fortunately, the probability of forging a cryptographic signature mechanism is computationally infeasible. So the output configuration of both the real-world and the ideal-world models are identical, that is, $\text{Out}^\text{ideal}_{\text{conf},A'} = \text{Out}^\text{real}_{\text{conf},A}$.

### 6. Simulation Results

In this section, we present the simulation results of SEMRAW. The results are compared with SODMRP [17], a popular secure multicast routing protocol based on on-demand multicast routing protocol (ODMRP). SODMRP is a detection (and reaction) based security protocol that identifies attacker nodes based on their forwarding behavior in the network. Even though such a protocol would not be the first choice to compare with a prevention based mechanism like SEMRAW, to the best of our knowledge we could not find another alternate multicast protocol that employs a prevention based approach. At first, the performance of both the protocols is compared for packet delivery ratio (PDR) in presence of malicious nodes, and later for the additional overhead incurred to provide security.

The experiments were carried out on OMNeT++ 4.2.1, a discrete event network simulator [37]. The network set-up consists of varying number of MRs (50–100) for different experiments, forming the mesh backbone. The transmission range of a MR is set to 100 m. MRs implement the 802.11s MAC protocol with a channel data rate of 54 Mbps. Source (or root of the tree) and multicast receivers are selected at random for each experiment. The simulation is repeated for randomly generated seed values, and the average results are plotted in the graphs.

Figure 2 shows the performance comparison of SEMRAW and SODMRP in presence of varying number of malicious nodes, in terms of percentage of packet delivered. The network set-up consists of 100 MRs distributed over an area of 1000 m$^2$. Randomly selected source nodes transmit CBR (constant bit rate) data traffic over UDP to a set of randomly selected multicast receivers. Packet size was set to 1024 bytes. The simulations were run for 500 seconds. Over time, different multicast sources become active to send 1 MB of data traffic (=100 data packets) to different receivers. Malicious nodes are strategically selected in such a way that they could affect more number of data flows in the network. Malicious nodes actively try to disrupt network services by launching attacks like metric manipulation attack, route corruption attack, and replay and wormhole attack. The principle goal of these malicious nodes is to degrade network performance and disrupt network services by dropping data packets.

SODMRP, similar to SEMRAW, relies on Join Query and Join Reply phase, where the multicast receivers broadcast their join tables to establish multicast routes to the source. SODMRP employs a reactive based approach to detect an attack. Each node that is part of the multicast forwarding group continuously monitors the discrepancy between effective PDR (ePDR) and perceived PDR (pPDR) and the route is considered to be under attack if $\text{ePDR} - \text{pPDR} > \delta$. ($\delta$ is the predefined detection threshold) A downstream
monitoring node on detecting malicious behavior accuses the upstream suspected node by flooding an accusation message that contains its identity and the identity of the accused node, as well as the duration of the accusation. For the duration of accusation the accused node would not be considered in route selection process. Figure 2 shows that SEMRAW performs better compared to SODMRP. Since SODMRP employs a reactive based approach it suffers from initial packet losses till the malicious behavior of an attacker node is detected.

Our later experiments were carried out to compute the overhead incurred by SEMRAW and SODMRP due to their respective security enhancements. First, we study the route creation overhead (in terms of additional bytes per packet) incurred for varying number of malicious attacker nodes. The network set-up comprised of 100 MRs spread over 1000 m². Figure 3 shows the overhead of SEMRAW in comparison to SODMRP. SEMRAW incurs constant overhead (in terms of additional bytes) as it requires three additional addresses to identify a wormhole link. Overhead of SEMRAW remains constant, irrespective of the number of malicious nodes as it employs a preventive based approach and the security scheme does not change with increase in the number of attackers. Therefore, when the network is free of attackers, SODMRP incurs less overhead compared to SEMRAW. However, with the increase in number of attackers SODMRP requires broadcasting accusation messages (contains identities of the accuser and suspected node, and the duration of accusation) across the network that requires additional bytes. With increase in number of attackers, higher number of accusation messages need to be transmitted and therefore incur more overhead than SEMRAW.

Finally, we compare the computation overhead in terms of signatures for SEMRAW and SODMRP for varying number of malicious nodes in a network of 50 MRs and a fixed average length of the route of 5. Figure 4 shows that with increasing number of attacker nodes the number of signatures required to protect messages in SODMRP is much higher compared to SEMRAW. It should be noted that, by increasing the number of malicious nodes in the network, we equally increase the number of source nodes that request for data transmission. SEMRAW requires two signatures per packet irrespective of the number of attacker nodes in the network. Therefore, the linear increase in total number of signatures in SEMRAW is due to increase in number of simultaneous multicast route formation processes. But on the other hand number of signatures in SODMRP increases with the increase in number of attacker nodes as more number of accusation messages are generated. Each node that generates an accusation message needs to sign it, so that the receiving node can appropriately verify it for authenticity. Thus, more attackers simply mean more number of accusation messages which result in more signatures.
### 7. Discussion

SEMRAW is the secure version of our multicast routing algorithm EMRAW [18]. The proposed algorithm preserves the performance merits of EMRAW as such, by selecting paths that incur fewer number of transmissions and establishing a bandwidth minimal multicast tree.

To address the security requirements, SEMRAW employs an integrated security framework to defend against all known active threats in multicast routing environment. It uses digital signatures to prevent attacks that involve malicious manipulations while it employs a wormhole detection mechanism to distinguish real links from wormhole links. The authenticated metric field protects mutable content in the JRQ and JRP message, thereby allowing the source and receivers to construct a secure multicast tree. SEMRAW allows an intermediate node to verify the content of routing messages in two steps. First, a node verifies the authenticity of the authenticated metric field appended by 2-hop node. This represents the cumulative content along the traversed path, acting as a check point. Secondly, it verifies the authenticity of the authenticated metric field appended by the previous hop. These two steps restrict intermediate nodes from acting on contents appended by previous hops, thus completely securing the multicast tree formation. In other words, each node acts as a check point that allows downstream nodes to verify the authenticity of multicast routing messages. Since each node verifies the validity of the path traversed by a routing message, it is infeasible for an attacker to launch an attack without being detected by a processing node.

The wormhole detection mechanism employed by SEMRAW works concurrently in conjunction with the tree selection mechanism. It facilitates nodes to monitor their two-hop subpaths and selects only such routes that are verified to be wormhole-free. It relies on the observations made in [36] to distinguish out-of-band links from real links. It relies on the fact that, in a uniformly distributed network, alternate routes within a maximum of 4-hops exist between node separated by a distance of $2R$, where $R$ is the transmission range of a node. However, SEMRAW is not without any limitations as any other algorithm. It requires the minimum length of wormhole link to be greater than $2R$ to successfully distinguish real links from wormholes. Since wormhole links of length less than $2R$ have negligible impact on the tree construction process, we safely ignore this limitation.

SEMRAW incurs additional computation and message overhead over EMRAW. This additional overhead results from the signatures employed during the secure tree construction process and due to the presence of additional addresses to detect wormhole attack. All the intermediate nodes that participate in route discovery, sign tree selection elements: Join Request, join reply, and route commit messages. At any instance, the Join Request (or join reply) element contains the signatures of the one-hop and two-hop nodes. Each intermediate node verifies the signatures of its immediate neighbor and its two-hop node, which adds to the computation overhead. Also, each intermediate node processes the addresses of previous hops for detecting wormhole links, adding to overhead in computations. Similarly, the presence of previous and current hop signatures slightly increases the message overhead. The presence of separate metric field increases the size of a message by a byte. However, the majority of the additional message overhead is due to the addresses of previous 4 hops for detecting wormhole links. Any intermediate node that receives a Join Request (or join reply) signs the path-selection element and the metric field separately and updates the addresses, before propagating it further into the network. Even though SEMRAW incurs additional overhead, the security provided by SEMRAW in an open operating environment of WMN outweighs this additional overhead.

Table 1 presents a security comparison of various existing unicast and multicast protocols. It can be observed that none of the existing protocols are secure against all known active attacks in wireless mesh network. Multicast routing protocols like BMSR [16] and SODMRP [17] can defend against Byzantine attacks, but they are essentially detection schemes that suffer from initial packet losses.

### 8. Conclusion

Securing multicast communications is essential to meet the performance requirements of wireless mesh network. In this paper, we proposed a secure multicast routing algorithm SEMRAW, to defend against all known active threats including wormhole attack. The security of the proposed protocol is analysed using simulation paradigm approach, which confirms its resistance against different active threats in a multicast routing environment. Later, the performance of SEMRAW is compared with a detection based protocol

### Table 1: Security comparison of different protocols.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Metric manipulation attack</th>
<th>Route corruption attack</th>
<th>Routing loop attack</th>
<th>Wormhole attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAODV [5]</td>
<td>Resistant</td>
<td>Not resistant</td>
<td>Resistant</td>
<td>Not resistant</td>
</tr>
<tr>
<td>ARAN [6]</td>
<td>Resistant</td>
<td>Not resistant</td>
<td>Not resistant</td>
<td>Not resistant</td>
</tr>
<tr>
<td>Ariadne [11]</td>
<td>Resistant</td>
<td>Not resistant</td>
<td>Resistant</td>
<td>Not resistant</td>
</tr>
<tr>
<td>SRP [12]</td>
<td>Not resistant</td>
<td>Not resistant</td>
<td>Resistant</td>
<td>Not resistant</td>
</tr>
<tr>
<td>SODMRP [17]</td>
<td>Resistant</td>
<td>Not resistant</td>
<td>Not resistant</td>
<td>Not resistant</td>
</tr>
<tr>
<td>EMRAW [18]</td>
<td>Not resistant</td>
<td>Not resistant</td>
<td>Not resistant</td>
<td>Not resistant</td>
</tr>
<tr>
<td>SEMRAW</td>
<td>Resistant</td>
<td>Resistant</td>
<td>Resistant</td>
<td>Resistant</td>
</tr>
</tbody>
</table>
SODMRP in terms of packet delivery ratio and additional overhead incurred to provide security.

**Competing Interests**

The authors declare that they have no competing interests.

**References**


