Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2016, Article ID 1563464, 11 pages
http://dx.doi.org/10.1155/2016/1563464

Research Article

Secure Multicast Routing Algorithm for Wireless Mesh Networks

Rakesh Matam[1] and Somanath Tripathy[2]

[1]*Indian Institute of Information Technology, Guwahati, Assam 781001, India*
[2]*Indian 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

Academic Editor: Shlomi Arnon

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 any time [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. BSMR 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 BSMR 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 $\Phi(v) \nsubseteq \Phi(v^*)$ 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 routing tables of all noncompromised nodes. A routing entry in v's routing table can be represented as a five-tuple field $(v, l_{\text{tar}}, l^1_{\text{nxt}}, l^2_{\text{nxt}}, C)$ in Q with identifier l_{tar} as target and l^1_{nxt} as the one-hop and l^2_{nxt} 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 noncompromised nodes are correct; that is, if v has a verified routing entry for target l_{tar} with one-hop l^1_{nxt} and two-hop l^2_{nxt} with cost C, then actually there exists a route that starts at node v and ends at node l_{tar} and the path through l^1_{nxt}, l^2_{nxt} 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 $(v, l_{\text{tar}}, l^1_{\text{nxt}}, l^2_{\text{nxt}}, C) \in Q$, 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) $l^1_{\text{nxt}} \in \ell(v_2)$,

(iv) $l^2_{\text{nxt}} \in \ell(v_3)$,

(v) $(l^1_{\text{nxt}}, l^2_{\text{nxt}}) \in E$,

(vi) $\sum C_{\text{link}} \leq C$.

3.4. Dynamic Representation of the System

3.4.1. Simulation Paradigm. SEMRAW is evaluated by simulation paradigm approach. The main idea of simulation-based approach is to construct two models, a real-world model and an ideal- world model to evaluate a protocol under investigation. A real-world model describes the operation of the protocol with all its details in a particular computational model whereas an ideal-world model describes the protocol in an abstract way mainly focusing on the services that the protocol should provide. Once constructed, the security of a real-world protocol is compared to that of an ideal-world implementation of the same task.

Both the models contain adversaries and their behavior is not constrained apart from the requirement that it has to run in polynomial time. The presence of an adversary in an ideal-world model essentially has no effect on the system due to the nature of its design. In other words, the ideal-world system is secure by its construction. The real-world model implements the actual protocol under consideration. Once both the models are implemented, the goal is to prove that for any real-world adversary there exists an ideal-world adversary that can achieve the same effects in the ideal-world model as those achieved by the real-world adversary in the real-world model. The security of a protocol interpreted from an adversary's generated view states that if the view generated by an adversary after executing a protocol in the real-world model can be solely generated from the information it legitimately possesses, then the protocol is termed to be secure. This implies that an adversary cannot gain extra information from the execution of a protocol, and everything that an adversary gathers can be generated by the adversary itself.

The real-world and ideal-world models are constructed as interacting Turing machines. The real-world model consists of honest and adversarial nodes represented by M_i and A_i, respectively. The nodes run the desired actual protocol in order to complete a specific task. Similarly, The ideal-world model too consists of honest and adversarial nodes, but the honest nodes interact with an ideal functionality F, running the ideal protocol ϕ. The functionality F is synonymous to the protocol to be evaluated, but it is provided with all the initial conditions that allows it to detect when the system goes into an incorrect state. An adversary in the ideal-world cannot gain any extra knowledge except for the information that F chooses to provide.

Definition 2 (statistical security). A routing protocol is said to be statistically secure if, for any configuration conf and any real-world adversary A, there exists an ideal-world adversary A' such that $\text{Out}^{\text{real}}_{\text{conf},A} \cong \text{Out}^{\text{ideal}}_{\text{conf},A'}$, where "$\cong$" means "statistically indistinguishable."

Intuitively, a routing protocol is said to statistically secure if the effect of a real-world adversary on a real-world 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 A are represented by K^u_A and K^v_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:

$$S \longrightarrow * : \{\text{JRQ}, \text{2HA}, \text{3HA}, \text{4HA}\}\, K^v_S \{M_S, \text{HC}, S\_\text{SQ}\}\, K^v_S. \quad (1)$$

JRQ represents the contents of the JRQ element. The 2HA represents the address of previous hop from which

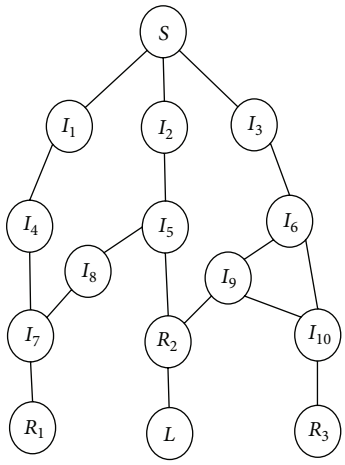

Figure 1: An example network connection.

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 proof of concept is presented in [36]. SEMRAW thrives on the fact that 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_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_1 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_1 then compares the two-hop address present in JRQ with the two-hop addresses of a set of existing routing entries represented by $\{\text{JRQ}_O\}$. 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 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_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:

$$I_1 \longrightarrow * : \{\text{JRQ}, S, \text{3HA}, \text{4HA}\}\, K^{v}_{I_1} \{M_S, \text{HC}, S\_\text{SQ}\}\, K^{v}_{S} \left\{M_{I_1}, \text{HC}, S\_\text{SQ}\right\} K^{v}_{I_1}. \quad (2)$$

Similarly, I_2 and I_3 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_5 from I_2 and I_6 from I_3) verifies the authenticity of the JRQ and the authenticated metric field appended by S and I_1. 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

$$I_1 \longrightarrow * : \left\{\text{JRQ}, S, I_1, \text{4HA}\right\} K^{v}_{I_4} \left\{M_{I_1}, \text{HC}, S\_\text{SQ}\right\} K^{v}_{I_1} \left\{M_{I_4}, \text{HC}, S\_\text{SQ}\right\} K^{v}_{I_4}. \quad (3)$$

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*

Reply (JRP). If a receiver receives multiple copies of the same *Join Request* from different neighbors, a route selection decision is made in favour of the node that offers better metric. A *Join Reply* is broadcasted by a receiver after a corresponding stable route entry has been created.

The JRP requires additional address fields to store the addresses of multicast receiver and the selected next-hop node towards the source. Two important fields, hop count (HC) and effective hop count (EHC), are introduced in *Join Reply* packet. The effective hop count (EHC) allows a node to compute effective distance from a receiver. The hop count is set to the value received in *Join Request* and EHC is set to 0 by a multicast receiver broadcasting the *Join Reply*. The EHC field of JRP is added to the authenticated metric field to prevent from malicious manipulation. The JRP broadcasted by R_1 is given by

$$R_1 \longrightarrow * : \{\text{JRP}, \text{2HA}, \text{3HA}, \text{4HA}\}\, K^{v}_{R_1} \left\{M_{R_1}, \text{HC}, \text{EHC}, D\_\text{SQ}\right\} K^{v}_{R_1}. \tag{4}$$

Processing of Join Replies by intermediate nodes varies depending on the type of node that receives the *Join Reply*. The proposed algorithm categorizes intermediate nodes into one of the two types: *free nodes and potential forwarders*. Nodes that are not part of the forwarding process for the current multicast tree are called *free nodes*, whereas a *potential forwarder* is a node that has been selected as forwarder by a receiver and awaits final confirmation from the source. In other words, a potential forwarder is a node that has recently received a *Join Reply* with next-hop address matching its own address. On receiving a nonduplicate *Join Reply*, a node I initially checks for the address present in next-hop (NH) address field. If it matches with its own address, a corresponding routing entry is created and thereafter I becomes a potential forwarder for that particular multicast group. The *Join Reply* is broadcasted after appropriately setting the next-hop address, hop count, and effective hop count. A *Join Reply* is considered original (not-duplicate) by a node only if it has not processed a similar *Join Reply* for a particular receiver.

A free node that receives a broadcasted *Join Reply*, compares the hop count and effective hop count values after decrementing and incrementing them, respectively. A *Join Reply* is broadcasted further only if HC $\geq$ EHC; else it is suppressed. Similarly, a potential forwarder receiving a broadcasted *Join Reply* increments the hop count, leaving the effective hop count unaltered. It propagates the received *Join Reply* through the established route towards the source. This allows a source node S to realize the existence of an alternate path that minimizes overall transmission count.

Similar to request phase, each intermediate node verifies the authenticity of signed JRP messages and metric fields. It appends a new authenticated metric field by discarding the old field appended by the two-hop node. Each node also verifies for the presence of out-of-band links by using the real-link detection mechanism discussed in the request phase.

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

$$S \longrightarrow I_2 : \{\text{RCOM}\}\, K^{v}_{S}. \tag{5}$$

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_5 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 ($\text{Out}^{\text{ideal}}_{\text{conf},A'}$) of the ideal-world model for ideal-world adversary A' is statistically indistinguishable from the output of a real-world model ($\text{Out}^{\text{real}}_{\text{conf},A}$) for any adversary A. In this case, $\text{sys}^{\text{real}}_{\text{conf},A}$ and $\text{sys}^{\text{ideal}}_{\text{conf},A'}$ 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 $(l_{\text{tar}}, l^1_{\text{nxt}}, l^2_{\text{nxt}}, C)$ for a target l_{tar} only if it has received a signed JRQ message which has been traversed through l^2_{nxt} and l^1_{nxt} with metric equal to C and the edge $(l^2_{\text{nxt}}, l^1_{\text{nxt}}) \in E$.

Now, the node v shares one-hop and two-hop neighborhood relations with l^1_{nxt} and l^2_{nxt}. 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_{tar}, but attacker forces l_{tar} to accept the corresponding message.

Case 2. There are routes from v to a node that uses the label l_{tar} going through the one-hop and two-hop neighbors l^1_{nxt} and l^2_{nxt} of v. But the link between $(l^1_{\text{nxt}}, l^2_{\text{nxt}}) \notin E$. 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_{tar}, but the sequence number received in the message through (l^1_{nxt} and l^2_{nxt} 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_{tar} going through l^1_{nxt} and l^2_{nxt} 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 force 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^2_{nxt} within a maximum of 4-hops, provided l^2_{nxt} 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^2_{nxt} and l^1_{nxt}. 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^1_{nxt} 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^2_{nxt} and l^1_{nxt} 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^2_{nxt} cannot be acted upon by l^1_{nxt} without forging the signature of l^2_{nxt}. 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 ePDR − pPDR > δ. (δ is the predefined detection threshold) A downstream

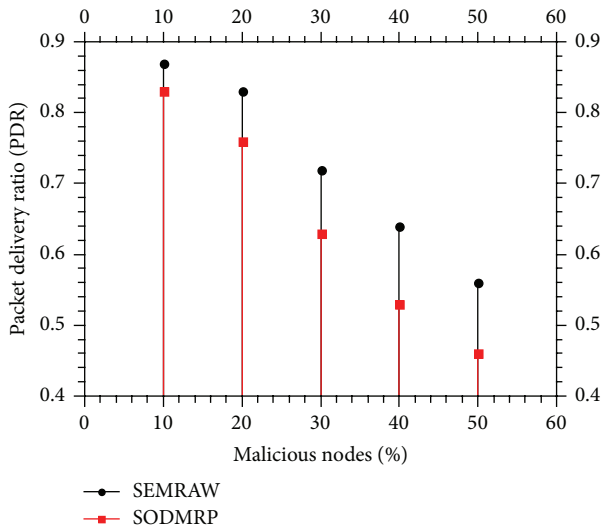

Figure 2: Performance comparison in terms of PDR.

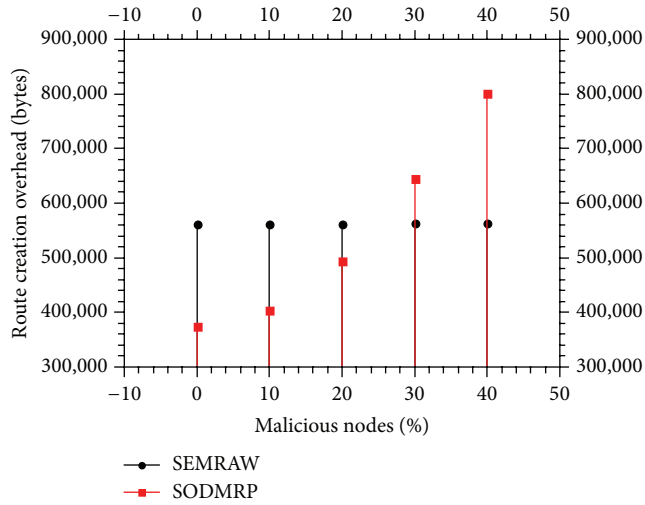

Figure 3: Route creation overhead for varying number of malicious nodes.

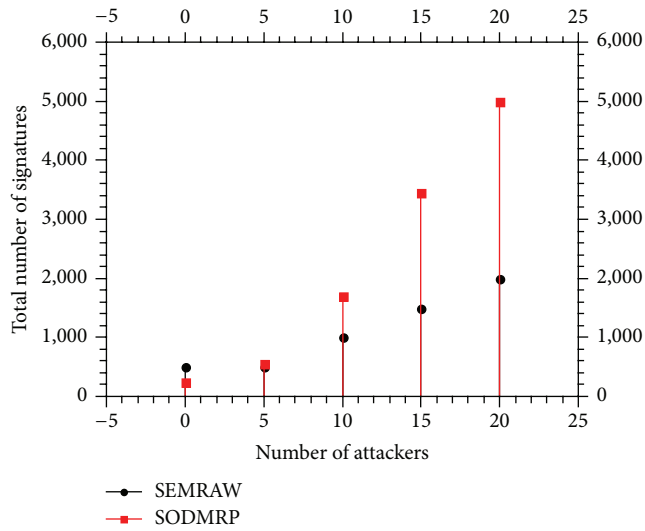

Figure 4: Signature overhead for varying number of attacker nodes.

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 m^2. 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.

Table 1: Security comparison of different protocols.

Protocol	Metric manipulation attack	Route corruption attack	Routing loop attack	Wormhole attack
SAODV [5]	Resistant	Not resistant	Resistant	Not resistant
ARAN [6]	Resistant	Not resistant	Not resistant	Not resistant
Ariadne [11]	Resistant	Not resistant	Resistant	Not resistant
SRP [12]	Not resistant	Not resistant	Resistant	Not resistant
SODMRP [17]	Resistant	Not resistant	Resistant	Not resistant
EMRAW [18]	Not resistant	Not resistant	Not resistant	Not resistant
SEMRAW	Resistant	Resistant	Resistant	Resistant

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 checkpoint 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 overweighs 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

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

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer Networks*, vol. 47, no. 4, pp. 445–487, 2005.

[2] P. A. K. Acharya and E. M. Belding, "MARS: link-layer rate selection for multicast transmissions in wireless mesh networks," *Ad Hoc Networks*, vol. 9, no. 1, pp. 48–60, 2011.

[3] N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, J. Wang, and D. P. Agrawal, "Wireless mesh networks: current challenges and future directions of web-in-the-sky," *IEEE Wireless Communications*, vol. 14, no. 4, pp. 79–89, 2007.

[4] S. Paul, *Multicast on the Internet and Its Applications*, Kluwer Academic, New York, NY, USA, 1998.

[5] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of the ACM Workshop on Wireless Security (WiSE '02)*, pp. 1–10, Atlanta , Ga, USA, September 2002.

[6] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP '02)*, pp. 78–87, IEEE, Paris, France, November 2002.

[7] R. Kravets, S. Yi, and P. Naldurg, "A security-aware routing protocol for wireless ad hoc networks," in *Proceedings of the ACM Symposium on Mobile Ad-Hoc Networking and Computing*, Long Beach, Calif, USA, October 2001.

[8] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, pp. 90–100, New Orleans, La, USA, February 1999.

[9] E. M. Royer and C. E. Perkins, "Multicast operation of the ad-hoc on-demand distance vector routing protocol," in *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, pp. 207–218, August 1999.

[10] S.-J. Lee, W. Su, and M. Gerla, "On-demand multicast routing protocol in multihop wireless mobile networks," *Mobile Networks and Applications*, vol. 7, no. 6, pp. 441–453, 2002.

[11] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," in *Proceedings of The 8th Annual International Conference on Mobile Computing and Networking (Mobicom '02)*, pp. 12–23, September 2002.

[12] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad-hoc networks," in *Proceedings of the SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS '02)*, San Antonio, Tex, USA, January 2002.

[13] D. Johnson and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for mobile ad hoc networks for IPv4," Tech. Rep., 2007, http://tools.ietf.org/html/RFC4728.

[14] C. W. Wu and Y. C. Tay, "AMRIS: a multicast protocol for ad hoc wireless networks," in *Proceedings of the IEEE Conference on Military Communications*, pp. 25–29, Atlantic City, NJ, USA, 1999.

[15] G. Acs, L. Buttyan, and I. Vajda, "Provably secure on-demand source routing in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 11, pp. 1533–1546, 2006.

[16] R. Curtmola and C. Nita-Rotaru, "BSMR: byzantine-resilient secure multicast routing in multihop wireless networks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 4, pp. 445–459, 2009.

[17] J. Dong, R. Curtmola, and C. N. Rotaru, "Secure high-throughput multicast routing in wireless mesh networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 5, pp. 653–668, 2011.

[18] R. Matam and S. Tripathy, "Improved heuristics for multicast routing in wireless mesh networks," *Wireless Networks*, vol. 19, no. 8, pp. 1829–1837, 2013.

[19] T. R. Andel and A. Yasinsac, "Adaptive threat modeling for secure Ad Hoc routing protocols," *Electronic Notes in Theoretical Computer Science*, vol. 197, no. 2, pp. 3–14, 2008.

[20] T. R. Andel and A. Yasinsac, "Surveying security analysis techniques in MANET routing protocols," *IEEE Communications Surveys and Tutorials*, vol. 9, no. 4, pp. 70–84, 2007.

[21] R. Matam and S. Tripathy, "Provably secure routing protocol for wireless mesh networks," *International Journal of Network Security*, vol. 16, no. 3, pp. 168–178, 2014.

[22] M. Burmester and B. D. Medeiros, "Towards provable security for route discovery protocols in mobile ad hoc networks," *IACR Cryptology ePrint Archive*, 2007.

[23] G. Ács, L. Buttyán, and I. Vajda, "Provable security of on-demand distance vector routing in wireless ad hoc networks," in *Security and Privacy in Ad-Hoc and Sensor Networks*, R. Molva, G. Tsudik, and D. Westhoff, Eds., vol. 3813 of *Lecture Notes in Computer Science*, pp. 113–127, 2005.

[24] L. Mao and J. Ma, "Towards provably secure on-demand distance vector routing in MANET," in *Proceedings of the International Conference on Computational Intelligence and Security (CIS '08)*, pp. 417–420, Suzhou, China, December 2008.

[25] Q. Niu, "Formal analysis of secure routing protocol for ad hoc networks," in *Proceedings of the International Conference on Wireless Communications and Signal Processing (WCSP '09)*, Nanjing, China, November 2009.

[26] L. Buttyán and T. V. Thong, "Formal verification of secure ad-hoc network routing protocols using deductive model-checking," in *Proceedings of the 3rd Joint IFIP Wireless and Mobile Networking Conference (WMNC '10)*, pp. 1–6, Budapest, Hungary, October 2010.

[27] S. Roy, D. Koutsonikolas, S. Das, and C. Hu, "High-throughput multicast routing metrics in wireless mesh networks," in *Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS '06)*, p. 48, IEEE, July 2006.

[28] Y. Li and I.-R. Chen, "Hierarchical agent-based secure multicast for wireless mesh networks," in *Proceedings of the IEEE International Conference on Communications (ICC '11)*, pp. 1–6, Kyoto, Japan, June 2011.

[29] J. Kim and S. Bahk, "Design of certification authority using secret redistribution and multicast routing in wireless mesh networks," *Computer Networks*, vol. 53, no. 1, pp. 98–109, 2009.

[30] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast," in *Proceedings of the Network and Distributed System Security Symposium (NDSS '01)*, San Diego, Calif, USA, February 2001.

[31] Y. Han, X. Gui, X. Wu, and X. Yang, "Proxy encryption based secure multicast in wireless mesh networks," *Journal of Network and Computer Applications*, vol. 34, no. 2, pp. 469–477, 2011.

[32] S. Zhao, A. Aggarwal, S. Liu, and H. Wu, "A secure routing protocol in proactive security approach for mobile ad-hoc

networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '08)*, pp. 2627–2632, IEEE, April 2008.

[33] P. M. Ruiz and A. F. Gomez-Skarmeta, "Heuristic algorithms for minimum bandwith consumption multicast routing in wireless mesh networks," in *Ad-Hoc, Mobile, and Wireless Networks*, V. R. Syrotiuk and E. Chávez, Eds., vol. 3738 of *Lecture Notes in Computer Science*, pp. 258–270, 2005.

[34] R. Mukherjee and J. W. Atwood, "Scalable solutions for secure group communications," *Computer Networks*, vol. 51, no. 12, pp. 3525–3548, 2007.

[35] H. Wang, Z. Cao, and L. Wei, "A scalable certificateless architecture for multicast wireless mesh network using proxy re-encryption," *Security and Communication Networks*, vol. 7, no. 1, pp. 14–32, 2014.

[36] R. Matam and S. Tripathy, "WRSR: wormhole resistant secure routing for wireless mesh networks," *Eurasip Journal of Wireless Communications and Networking*, vol. 2013, article 180, 2013.

[37] The OMNeT++ Network Simulator, http://www.omnetpp.org.