Hierarchical Agent-Based Secure and Reliable Multicast in Wireless Mesh Networks

Yinan Li*, Ing-Ray Chen*

Abstract

We propose and analyze a hierarchical agent-based secure and reliable multicast (HASRM) algorithm for efficiently supporting secure and reliable mobile multicast in wireless mesh networks, with design considerations given to minimize the overall network cost incurred by reliable multicast packet delivery, mobility management, security key management, and group membership maintenance. HASRM dynamically maintains a group of multicast agents running on mesh routers for integrated mobility and multicast service management and leverages a hierarchical multicast structure for secure and reliable multicast data delivery. The regional service size of each multicast agent is a key design parameter. We show via model-based performance analysis and simulation validation that there exists an optimal regional service size that minimizes the overall communication cost and the optimal regional service size can be dynamically determined. We demonstrate that HASRM under optimal settings significantly outperforms traditional algorithms based on shortest-path multicast trees extended with user mobility, security, and reliability support. We also show that a variant of HASRM is superior to a recently proposed multicast algorithm for secure group communication in wireless mesh networks.

Key Words: Group communications; mobile multicast; security; reliability; wireless mesh networks; performance analysis

*Department of Computer Science; Virginia Tech; Northern Virginia Graduate Center; Falls Church, VA 22043, USA; email: {yinan926, irchen}@vt.edu.

1 Introduction

Wireless mesh networks are widely regarded as a cost-effective solution for next generation last-mile wireless Internet access. A wireless mesh network (WMN) consists of two types of components: wireless mesh routers (MR) and mesh clients (MC) [1]. MRs typically form a static mesh networking infrastructure called a wireless mesh backbone serving MCs that are end-user mobile devices with wireless access capability. A WMN is also typically interconnected with the Internet through a gateway, which is a special MR that performs the gateway/bridge function.

Group communications based on multicasting is expected to be a common communication paradigm in WMNs, due to the broadcasting nature of wireless communications and the community-oriented nature of WMNs [2]. In this paper, we investigate the problem of supporting secure and reliable mobile multicast services in WMNs, and propose an efficient algorithm called Hierarchical Agent-based Secure and Reliable Multicast (HASRM). We identify the following requirements that HASRM must fulfill:

- The algorithm must take security measures to ensure that only authenticated members in a multicast group have access to the multicast data at any time. Particularly the algorithm must guarantee *forward secrecy* and *backward secrecy*. Secure multicast has received intensive attention due to its importance to group communications. It is particularly critical in WMNs because of the openness of wireless communications.

- The algorithm must handle failures of unreliable wireless links efficiently to guarantee that all group members receive each multicast packet. This guarantee is necessary for applications that require reliable multicast services, e.g., electronic newspaper and magazine delivery, and multi-site business data distribution.

- The algorithm must handle user mobility efficiently and support *mobile multicast* such that group members can receive multicast data when they move and change their locations (in terms of serving MRs) frequently. User mobility support is critical in WMNs because MCs, which are end-user mobile devices, can have frequent movement.

The most salient feature of HASRM is that it addresses *integrated user mobility, secure and reliable multicast service management*. To the best of

our knowledge, HASRM is the first multicast algorithm proposed for WMNs that provides both security and reliability support to mobile users. HASRM follows the design principle of *integrated mobility and service management for network cost minimization*, and is designed for providing *secure and reliable* multicast services to mobile users in WMNs, explicitly taking the effect of user mobility into consideration. We emphasize integrated mobility and service management for network cost minimization for the following reasons:

- User mobility can have a significant impact on multicast service management. For example, the group multicast tree may need to be updated from time to time to maintain its structural properties when group members are mobile.
- Performance optimization that only takes multicast service management itself into consideration may adversely lead to excessive overhead when users are mobile.
- Minimizing the overall network cost incurred has positive impact on other performance metrics, such as throughput, delay, packet delivery ratio, etc.

HASRM is a decentralized hierarchical algorithm [3] by which a single multicast group is divided into subgroups managed locally by entities called *multicast agents* (MA). Rekeying of security keys and group membership management are largely localized within the service region of an MA. An MA *is* an MR that besides being a regular wireless mesh router, also acts as a point of regional registration for integrated mobility and multicast service management following the design idea of micro-mobility management [4, 5, 6, 7, 8]. A multicast group member at all time is associated with a single MA, but changes its MA and thus moves to another service region from time to time based on its mobility and multicast service characteristics. On the other hand, an MA may service multiple members simultaneously. HASRM dynamically determines the optimal regional service size of an MA (i.e., the number of MRs covered by the MA) that minimizes the overall network cost, based on the multicast group service characteristics and group dynamics in terms of member mobility and membership changes. HASRM achieves cost minimization by balancing the tradeoff between the cost for reliable multicast data delivery vs. the signaling cost for security, group membership, and mobility management tasks.

We develop a mathematical model based on stochastic Petri nets [9, 10, 12, 13, 14, 15, 16, 17] to analyze the performance of HASRM with simulation validation, focusing on the effect of key parameters on the performance of HASRM. We demonstrate that HASRM under optimal settings (which can be derived dynamically using the proposed analytical model) significantly outperforms traditional algorithms based on shortest-path multicast trees extended with user mobility, security, and reliability support. We also compare HASRM with a recently proposed protocol framework for secure group communication in WMNs, called Secure Group Overlay Multicast (SeGrOM) [2]. We choose SeGrOM because it is also a hierarchical decentralized multicast algorithm based on a two-tier multicast structure. Like HASRM, it handles member mobility and dynamic group membership with decentralized management. We show that HASRM is superior to SeGrOM in terms of the overall network cost incurred by multicast data delivery, security key management, mobility management, and group membership management.

This paper extends from [18] which considers only secure multicast support. In this paper, HASRM is redesigned to also provide reliable multicast services to guarantee that all group members receive each multicast packet without unduly delay. The performance model developed in this paper thus considers integrated secure and reliable multicast service management. Moreover, a comparative analysis of HASRM against existing approaches as well as a sensitivity analysis of design parameters are conducted in this paper with simulation validation. We also discuss the practicality and implementation of HASRM on real mobile devices in this paper.

The remainder of this paper is organized as follows. Section 2 surveys existing work on secure and reliable multicast in wireless networks (including WMNs). Assumptions and system design goals in security and reliability are introduced in Section 3. Section 4 gives a detailed introduction to HASRM. In Section 5 we develop an analytical model for evaluating the performance of HASRM. Performance analysis and detailed comparison results are presented in Section 6 and Section 7. Section 8 presents simulation results. Issues related to the implementation of HASRM on real mobile devices are discussed in Section 9. The paper concludes with Section 10.

2 Related Work

There is a large body of existing work on supporting multicast services for mobile hosts in Mobile IP networks. The IETF Mobile IP specification [19] defined two standard approaches for supporting mobile multicast, namely, remote subscription (RS) and bi-directional tunneling (BT). In RS, whenever a mobile node (MN) enters into a foreign network, it performs a subscription to its multicast group in the foreign network. In this way, the optimal paths for multicast packet delivery are maintained in the presence of dynamic multicast group membership and topology due to membership changes and user mobility. A major drawback of RS is the large signaling overhead for multicast group subscription and multicast tree reconstruction. In BT, multicast packets are first intercepted by the HA of the MN, and subsequently delivered from the HA to the MN via standard Mobile IP tunnels. The advantage of BT is that the signaling overhead for multicast group subscription and multicast tree reconstruction is avoided. A major disadvantage, however, is that the paths for multicast delivery in BT are generally far from optimal.

Both RS and BT have advantages and disadvantages that are complementary. Based on the idea that the advantages of the two basic approaches can be combined to offer better efficiency and scalability, various hybrid approaches [20, 21, 22] have been proposed. RMMP [23] is a protocol that provides reliable multicast services in Mobile IP networks. RMMP is derived from the RS approach, and instead of requiring an MN to re-subscribe to the multicast group whenever it moves to a new foreign network, it requires the foreign agent to join the multicast group and aggregate feedbacks from MNs in its affiliated subnet.

Despite that a handful of algorithms exist for supporting mobile multicast services in Mobile IP networks, these algorithms cannot be applied to WMNs directly without major modification and performance penalty. For example, the lack of centralized management facilities such as home/foreign agents in Mobile IP networks makes these algorithms not directly applicable to WMNs, as argued in [1].

The research of multicast algorithms in WMNs is still in its infancy. Very recently a few multicast protocols have been proposed [24, 25, 26, 27], focusing on algorithms for multicast tree construction for maximizing the multicast throughput. Algorithms proposed for secure group communications in WMNs [28, 29, 30] generally considered the issues related to secure group key distribution and group key agreement. In [28], a method was proposed for

designing multicast key management trees that match the network topology to reduce the communication overhead associated with rekeying. A bandwidth efficient key tree management scheme was proposed in [29], focusing on assignment of key encryption keys (KEK) to newly joining members to reduce the bandwidth consumption. Group key agreement in WMNs was studied in [30] by comparing three different group key agreement protocols. Pacifier [31] is a recently proposed multicast protocol for WMNs that targets high throughput and reliability. Pacifier maintains an efficient multicast tree for tree-based opportunistic multicast routing to achieve high throughput, and utilizes intra-flow network coding to achieve high reliability.

To the best of our knowledge, none of these algorithms considered user mobility support and the implication of user mobility on multicast tree maintenance, reliable multicast data delivery, security key management, and performance optimization. Unlike existing algorithms, HASRM is designed for mobile users in a WMN who may have high mobility. HASRM takes into account the effect of user mobility on secure and reliable multicast service management using an integrated design and a performance measure that combines the cost for multicast service management and the signaling cost for mobility management.

Hierarchical reliable multicast (HRM) [32] refers to reliable multicast algorithms that partition a multicast group into subgroups and employ a proxy in each subgroup that manages reliable multicast locally. A proxy is responsible for caching multicast data packets, collecting feedbacks from the multicast receivers, and locally retransmitting data packets in case of losses. HASRM can be considered as an instance of HRM algorithms. Unlike the work in [32], which focuses on optimizing the placement of a fixed number of static proxies on a multicast tree, HASRM dynamically determines the optimal regional service size of an MA (similar to a proxy) to minimize the network cost.

3 Assumptions and Design Goals

We consider a multicast group that has a single source and dynamic group topology and membership in a WMN. The multicast source can be either a host in the Internet or an MC within a WMN. If the multicast source is an MC within a WMN, the backbone multicast tree is rooted at the source. On the other hand, if the source is a host in the Internet, the backbone multicast

tree is rooted at the gateway, as multicast packets will first be routed to the gateway which is responsible for delivering them to the group members.

The multicast group is dynamic with respect to group member locations because of user mobility and group membership because of member join and leave events. A multicast group may have high group dynamics in terms of both member locations and group membership, as reflected by the relevant parameter values given in Section 6. The multicast source on the other hand is assumed to be static.

Within the lifetime of a multicast group, a member may join or leave the group at arbitrary time. We assume that group member join and leave events can be modeled by Poisson processes with rates of λ and μ, respectively. That is, the inter-arrival and inter-departure times are exponentially distributed with averages $1/\lambda$ and $1/\mu$, respectively. We further assume that λ and μ have about the same value such that the multicast group size remains stable over time.

We assume that each MR possesses a pair of public/private keys and a public-key certificate that contains the identifier of the MR and its public key. There exists a central certificate authority (CA) in the WMN that is responsible for managing MR certificates. The gateway also stores the certificates and uses the public key of an MR to encrypt information (e.g., group key) to be sent to the MR.

We assume that the probability p of packet losses due to wireless link failures is known. HASRM achieves reliable multicast data delivery through NAK-based retransmissions [33]. Our failure model is mainly concerned with losses of multicast data packets due to mobility and unreliable wireless links. Failures of MRs are considered rare relatively to wireless link failures and are not treated.

The central security goal of HASRM is to provide data secrecy via encryption to protect multicast data from unauthorized access by adversaries outside the multicast group. Our security attack model considers only outside attackers. We do not consider insider attacks from entities within the multicast group. Specifically, HASRM needs to satisfy the forward and backward secrecy properties, i.e., it is computationally infeasible for a client to decrypt and read multicast data sent before it joins or after it leaves the multicast group. These two properties ensure that only authorized clients with a valid group membership have access to multicast data.

4 Hierarchical Agent-based Secure and Reliable Multicast

HASRM employs a two-level hierarchical multicast structure. At the upper level of the hierarchy is a backbone multicast tree, which is a source-rooted multicast tree connecting MRs that serve as MAs. The tree is updated when an MA joins or leaves due to user mobility and group membership changes. HASRM dynamically maintains a group of MRs serving as MAs for integrated user mobility and secure and reliable multicast service management. Each multicast group member is registered with and serviced by an MA from which it receives secure and reliable multicast service. The member also reports its updated location information to the MA, whenever it moves and changes its serving MR. Each MA maintains a table that stores the up-to-date location information (the address of the current serving MR) of each multicast group member it currently services.

An MA and those members it services essentially form a local multicast group at the lower level of the hierarchy. Each MA services a region covering a number of MRs. The regional service size of an MA is a key parameter controlling the tradeoff between the packet delivery cost and the signaling cost for various management tasks. There exists an optimal regional service size that minimizes the overall communication cost. We model the optimal regional service size by the optimal threshold for the number of hops a member can be away from its MA, denoted by $H_{optimal}$. This optimal threshold can be determined using the analytical model developed in Section 5. Let H and $H_{optimal}$ denote the threshold and the optimal threshold, respectively.

4.1 Security Key Management

Each multicast group member shares a pair-wise secret key K_u with its MA, which uses the key to securely deliver multicast packets to the member. K_u can be established using the Diffie-Hellman (DH) key exchange protocol [34]. Whenever the member changes its MA due to its mobility, a new K_u shared with the new MA is generated. The source and the group of MAs share a *group key* K_g for data encryption that is used to transmit multicast packets securely from the source to the MAs through the backbone multicast tree. To guarantee forward secrecy and backward secrecy, K_g must be updated every time an MA joins or leaves the backbone multicast tree.

- *MA join*: When an MA joins the backbone multicast tree, the old group key K_g is discarded and a new key K'_g is generated to ensure forward secrecy. The source and MAs currently in the multicast group generate K'_g in a distributed way by applying a one-way hash function h to K_g, i.e., $K'_g = h(K_g)$ [35]. Because the newly joining MA does not possess K_g, it cannot generate K'_g using this method. Instead, the source securely sends K'_g to the MA using its public key.

- *MA leave*: When an MA leaves the backbone multicast tree because it no longer services any multicast group member, K_g needs to be updated to offer backward secrecy. The source generates a new shared group key K'_g using the *key tree* approach [36] and distributes the key utilizing PKI to all MAs excluding the one that is leaving via *rekey* messages [36].

Table 1 summarizes the various security keys used in HASRM. HASRM uses conventional symmetric encryption and the DH protocol for key exchange to avoid the overhead associated with public-key encryption at the expense of the communication cost for key exchange. Considering that the packet rate is typically much higher than the mobility rate, the saving in the encryption/decryption cost is significant.

Table 1: Security keys used in HASRM.

Key	Meaning
K_g	The group key shared by the source and the group of MAs
K_m	The public key of an MA
K_u	The pair-wise secret key shared between a multicast group member and its MA

4.2 Reliable Multicast Data Delivery

The procedure for multicast data delivery when no failures of wireless links present is straightforward. The source first encrypts the packet using the group key K_g, and disseminates the encrypted packet to the subgroups (MAs) through the backbone multicast tree. Each MA, upon receiving the encrypted packet, decrypts the packet using the group key K_g, and re-encrypts the

packet using the pair-wise key K_u with a group member it serves in its service region, and then sends the new encrypted packet to this group member. The group member finally decrypts the packet using the pair-wise key K_u shared with its MA. Therefore, a complete multicast transmission from the source to a group member is a two-stage process and involves two pairs of encryption/decryption operations.

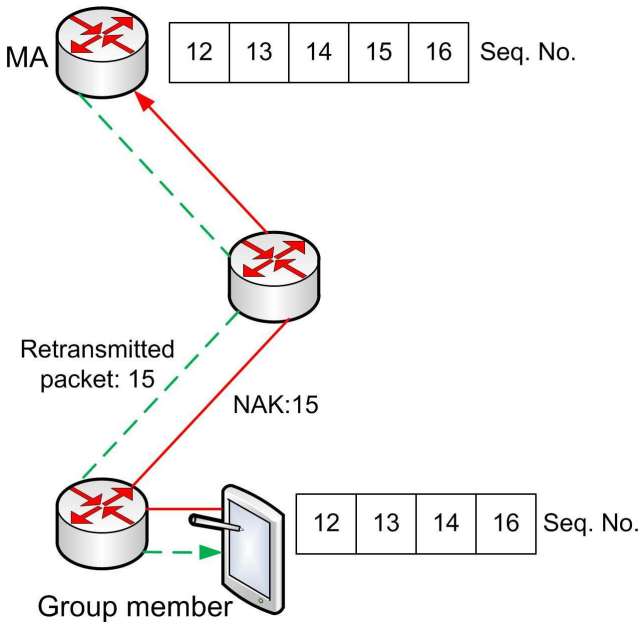

Figure 1: NAK-based retransmissions.

In the presence of failures of wireless links that cause multicast data packet losses, error recovery based on retransmissions is necessary to provide reliable multicast data delivery. Specifically, HASRM uses NAK-based retransmissions [33], i.e., a group member sends a negative acknowledgement when it missed a multicast data packet. Multicast data packet losses can be detected using gaps in the sequence numbers, as illustrated in Fig. 1. The following error recovery procedure is executed in case of packet losses:

- At the lower level of the hierarchy, when a multicast group member detects a multicast data packet loss, it sends a negative acknowledgement to its MA. The MA retransmits the lost packet to the group member when it receives the acknowledgement. Fig. 1 illustrates NAK-based

retransmissions at the lower level of the hierarchy. Therefore, multicast data packet losses occurring at the lower level of the hierarchy are handled locally within the service region of each MA. In addition, the MA discards a buffered data packet after a maximum period of time for late negative acknowledgements to arrive and it also aggregates acknowledgements to limit acknowledgement implosion, so as to save bandwidth.

- At the upper level of the hierarchy, when an MA detects a gap in the sequence numbers, i.e., a multicast data packet loss, it sends a negative acknowledgement to the source. The source needs to retransmit the lost packet to the MA upon receiving the acknowledgement. Two options are available for retransmissions [32]:

  - *Multicast*: the source retransmits the lost multicast packet by multicasting the packet to all MAs, regardless of whether they have already successfully received the packet or not.
  - *Unicast*: the source individually retransmits the multicast packet to each of the MAs that experienced the loss. MAs that successfully received the original packet will not receive the retransmitted one.

  Which option is better depends on the loss probability of wireless links. If the loss probability is high, such that the number of MAs experiencing losses are relatively large, the multicast option is better because the signaling overhead of individual unicast will be significant. On the other hand, if the loss probability is not significantly high, the unicast option is better. In this paper, we will only consider retransmissions based on unicast at the upper level of the hierarchy.

The lower level always uses unicast routing for multicast delivery from an MA to the group members associated with it. The reasons of using unicast routing at the lower level are as follows:

- The optimal service region size of an MA can be quite diverse for different group members depending on their diverse mobility and service characteristics. The result is that the wireless broadcast advantage is no longer valid, given that group members associated with the same MA (typically not a large number) can be highly dispersed in a large

service area around the MA. Consequently, the overhead of multicast routing can be considerably high. Thus, using broadcast routing at the lower level can adversely affect the communication cost.

- Using unicast routing at the lower tier eliminates the need for multicast tree maintenance at the lower level and simplifies mobility management. The need for mobility management as well as multicast tree maintenance would be frequent if multicast routing is used at the lower level, as multicast group members may have high mobility. If unicast routing is employed at the lower level, the overhead of multicast tree maintenance and multicast group membership management at the lower level would be completely eliminated. The saving can be significant, considering that group members can have high mobility and that the number of multicast groups at the lower level can be potentially large.

- Using unicast routing at the lower tier significantly reduces the overhead for error recovery from data packet losses at the lower tier. When a multicast member detects a data packet loss, it would send a negative acknowledgement to its MA. The MA would process the acknowledgement locally by retransmitting the lost packet to the member through unicast, without having to broadcast to all members under it through multicast.

In Section 7, we perform a comparative analysis of HASRM with SeGrOM [2], a hierarchical decentralized multicast algorithm based on a two-tier multicast structure, with simulation validation in Section 8 to justify our design choice.

It is also worth emphasizing that source-based retransmissions are only used at the higher level when an MA detects a data packet loss. At the lower level, however, multicast data packet losses and retransmissions are handled locally within the service region of each MA. As discussed above, when a multicast member detects a data packet loss, it would send a negative acknowledgement to its MA. The MA would process the acknowledgement locally by retransmitting the lost packet to the member, without relaying it to the source. Considering that the number of multicast group members is much larger than that of the MAs, this approach can significantly reduce the burden on the source.

4.3 Dynamic Group Membership Management

4.3.1 Member Join

To join a multicast group, an MC first selects a serving MR among all MRs within the wireless transmission range, say, based on the wireless link quality, and sends a *join request* to the selected MR. If the MR is not yet a part of the backbone multicast tree, it joins the backbone multicast tree by sending a join request to the source. The source computes a shortest path to the MR and sends a join acknowledgement along the path back to it. Any intermediate MR on the path that is not a node on the backbone multicast tree automatically becomes an on-tree node when it receives the join acknowledgement. The MR forwards the acknowledgement to the MC, confirming that it becomes a new member of the multicast group. When joining the multicast group, the MC executes the DH protocol with the new serving MR to generate a new K_u.

4.3.2 Member Leave

To leave a multicast group, a member has to notify its MA. After the member leaves, the MA may no longer service any multicast group member, and therefore it needs to be removed from the backbone multicast tree. The leaving member sends a leave request to its MA, which responds with a leave acknowledgement as a confirmation. If the MA needs to remove itself from the backbone multicast tree because it no longer services any group member, it forwards the leave request to the source, which then updates the backbone multicast tree and sends the MA an acknowledgement.

4.4 Mobility Management

In HASRM, when a member moves and changes its serving MR, the following procedure is executed to handle mobility and backbone multicast tree management:

- The member associates with the new serving MR by sending an association request to it. The MR responds with an association acknowledgement.
- If the new serving MR is not an MA and is within the service region of the member's MA, the member reports the serving MR change to its

MA by a location update message. If the new serving MR is already an MA, the member switches to the new MA and starts receiving multicast packets from the new MA.

- If the new serving MR is H hops away from the member's current MA, the threshold is reached and the new serving MR sends a join request to the source to join the backbone multicast tree and becomes the member's new MA.

- The member executes the DH protocol to generate a new key K_u when it associates with the MA.

- After being associated with the new MA, the member sends a deassociation request to its old MA, which responds with a deassociation acknowledgement. If the member's old MA no longer services any member, it removes itself from the backbone multicast tree by sending a leave request to the source.

5 Performance Model

In this section, we develop a stochastic Petri net (SPN) model for analyzing the performance of HASRM. Table 2 lists the parameters and their physical meanings used in performance modeling and analysis. The physical meaning of the mobility rate denoted by σ is the average number of serving MR changes made by a multicast group member per time unit. The time unit used in this paper is second. If a group member moves and changes its serving MR once every 10 minutes, its mobility rate is $\frac{1}{600}$. The physical meanings of other parameters are clear from the context.

We assume that the WMN has a two-dimensional $n \times n$ structure with wraparound on the boundary such that each MR has exactly four neighbors, as illustrated in Fig. 2. A multicast group member can move from its serving MR randomly to any of its four neighbors with equal probabilities. The average unicast path length denoted by α in this $n \times n$ mesh network model is given as $\alpha = \frac{2n}{3}$.

We model the process of arrival and departure of M multicast group members to and from an MR using an $M/M/\infty/M$ queue. Fig. 3 depicts the Markov chain for the $M/M/\infty/M$ queueing model. The probability P_0

Table 2: Parameters and their physical meanings.

Parameter	Physical meaning
σ	the mobility rate
λ_p	the multicast packet rate
λ	the rate of member join events
μ	the rate of member leave events
M	the multicast group size
n	the dimension of the WMN
α	the average unicast path length of the WMN
ω	the arrival rate of a single member to an arbitrary MR
P_{MA}	the probability that an arbitrary MR is also an MA
P_0	the probability that an MR is not covering any member
P_1	the probability that an MR covers exactly one member
P_1^{MA}	the probability that an MA services exactly one member
N_{MA}	the number of MAs
T	the multicast tree size in terms of the total number of tree nodes
κ	the multicast scaling factor
p	the loss probability of wireless links
P_h	the probability that a multicast data packet is successfully delivered along the path to a multicast group member from its MA which is h hops away
E_h	the expected number of retransmissions needed for an MA to deliver a multicast packet to a group member which is h hops away
L	the expected hop distance from the source to an MA
P_L	the probability that a multicast data packet is successfully transmitted from the source to an MA which is L hops away
E_L	the expected number of retransmissions needed for the source to disseminate a multicast packet to an MA which is L hops away

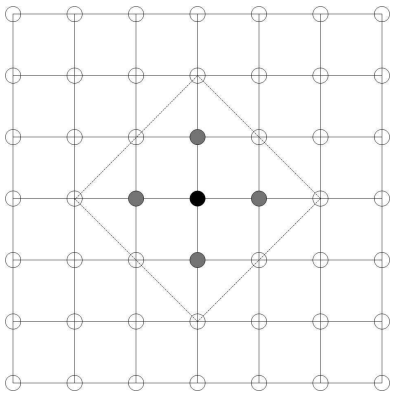

Figure 2: An $n \times n$ mesh network model.

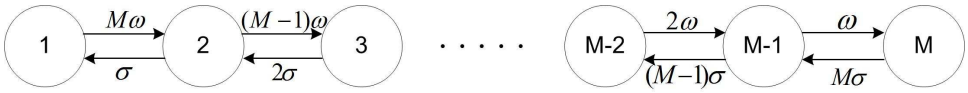

Figure 3: The Markov chain modeling the process of arrival and departure of M multicast group members to and from an MR.

that an MR is not servicing any group member and the probability P_1 that an MR services one member can be derived using the queueing model as:

$$\begin{array}{l} P_0 = (1 - \frac{1}{n^2})^M \\ P_1 = \frac{M}{n^2}(1 - \frac{1}{n^2})^{M-1} \end{array} \tag{1}$$

It can be shown that, given the distance threshold H, the number of MRs covered by the service region of an MA (an example is given by the dotted-line-bounded area in Fig. 2) on average is $2H^2 - 2H + 1$. The probability P_{MA} that an arbitrary MR is an MA is therefore given by:

$$P_{MA} = \frac{1}{2H^2 - 2H + 1} \tag{2}$$

An MA services exactly one member if all the MRs within its service region service just one member. Therefore, the probability P_1^{MA} that an MA services exactly one member can be calculated as:

$$P_1^{MA} = \binom{2H^2 - 2H + 1}{1} \cdot P_0^{2H^2 - 2H} \cdot P_1 \tag{3}$$

At the upper level of the hierarchy, the number of MRs comprising the backbone multicast tree can be derived using the following method. First, the ratio of the total number of multicast links (among MRs) on the tree denoted by L_m over the average unicast path length of the network denoted by α is given by a power-law [37, 38] as follows:

$$\frac{L_m}{\alpha} = R^{\kappa} \Rightarrow L_m = \alpha \cdot R^{\kappa} \tag{4}$$

where κ is the *multicast scaling factor*, and is found to be close to 0.7 [37]. R denotes the number of leaves on the multicast tree, i.e., the number of MAs, and is calculated as:

$$R = N_{MA} = P_{MA} \cdot N \tag{5}$$

Given L_m, the total number of MRs (including the MAs) on the backbone multicast tree denoted by T is given as:

$$T = L_m + 1 = \alpha \cdot (N_{MA})^{\kappa} + 1 \tag{6}$$

A multicast data packet is successfully delivered along the path from the MA to the member only if no links on the path lose the packet. Thus, the probability P_h that a multicast data packet is successfully delivered along the path to a multicast group member from its MA which is h hops away is calculated as follows:

$$P_h = (1 - p)^h \tag{7}$$

where p is the per-hop wireless link loss probability. Given P_h, the expected number of retransmissions needed for an MA to deliver a multicast packet to a group member which is h hops away, i.e., E_h, can be calculated as follows:

$$E_h = \frac{1}{P_h} = \frac{1}{(1 - p)^h} \tag{8}$$

The expected hop distance L from the source to an MA is calculated as the average length of paths from the source to the MAs, i.e., the average depth of the MAs (leaves) on the backbone multicast tree. Given that the number of tree nodes is T and let d denote the degree of inner nodes, L can be calculated as follows, assuming a perfectly balanced backbone multicast tree:

$$L = \log_d T \tag{9}$$

Given L, the probability P_L that a multicast data packet is successfully transmitted from the source to an MA which is L hops away from the source is given by:

$$P_L = (1-p)^L \tag{10}$$

The expected number of retransmissions E_L needed for the source to disseminate a multicast packet to an MA is given as follows:

$$E_L = \frac{1}{P_L} = \frac{1}{(1-p)^L} \tag{11}$$

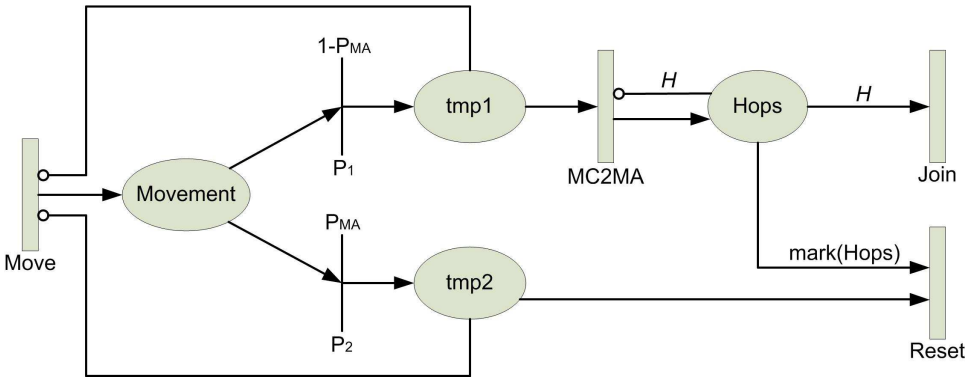

Figure 4: The SPN model for HASRM.

Here we present the SPN model for analyzing the performance of HASRM and particularly for determining the optimal threshold $H_{optimal}$. Fig. 4 shows the SPN model for describing the behavior of a single group member. An SPN model consists of places, tokens, and transitions (for modeling events). Table 3 explains the meanings of places and transitions defined in the SPN model. Here `mark(P)` is a function that returns the number of tokens in place `P`. A token in this model represents a location change, i.e., a change of the serving MR of the group member. The underlying model of our SPN model is a semi-Markov chain, which when solved, yields the probability that the group member is in a particular state. Below we explain how the SPN model is constructed.

- The event of member movement is modeled by transition *Move*, the transition rate of which is σ. When the member moves to and is associated with a new MR, a token is put into place *Movement*.

Table 3: The meanings of places and transitions defined in the SPN model for HASRM.

Symbol	Meaning
Movement	`mark(Movement)=1` means that the member moves to a new MR
Hops	`mark(Hops)` returns the number of hops the member is away from its MA
Move	A timed transition modeling the movement of the member
MC2MA	A timed transition modeling the regional location registration event
Join	A timed transition modeling that the new serving MR joins the multicast tree and becomes a new MA
Reset	A timed transition modeling the event triggered when the new serving MR is already an MA
H	The threshold for the number of hops a member can be away from its MA

- The new MR may be either an ordinary MR or an MA. The SPN model distinguishes between these cases using two immediate transitions *P1* and *P2* associated with probabilities $1 - P_{MA}$ and P_{MA}, respectively.
- In the first case that the new MR is not an MA, the member reports its new location to its MA. The event is modeled by transition *MC2MA*.
- After transition *MC2MA* is fired, a token is put into place *Hops*. The number of tokens denoted by *mark(Hops)* in place *Hops* represents the number of hops the member is away from its MA.
- When the number of tokens in place *Hops* reaches H, i.e., $mark(Hops) = H$, transition *Join* is fired, modeling that the new MR joins the backbone multicast tree and becomes the new MA for the member. The firing of transition *Join* resets the number of hops away from its current MA to zero. This is modeled by consuming all the tokens in place *Hops*.
- In the second case that the new MR is an MA, the member registers with the new MA, and the new MA replaces its old MA. This is modeled

by transition *Reset*, the firing of which consumes all the tokens in place *Hops*.

We use the *average total communication cost incurred per member per time unit* as the metric for performance evaluation and analysis. We define the total communication cost as the *total number of hops of wireless transmissions incurred*. For example, the service cost incurred per multicast packet delivery per member is given by the average number of hops traveled per packet from the source to any member. The reason we use this cost as the performance metric is that it reflects the network traffic load and, consequently, directly impacts traditional performance measurements such as throughput and latency.

Using the above metric, the average total communication cost incurred per member per time unit by HASRM, denoted by C_{HASRM}, includes the cost for reliable multicast packet delivery, the cost for mobility management, the cost for security key management, and the cost for group membership management. The service cost for reliable multicast packet delivery (C_s) consists of two parts. The first part (C_s^1) is for the transmissions/retransmissions at the upper level from the source to the MAs. The second part (C_s^2) is for the transmissions/retransmissions at the lower level from the MAs to the group members.

Assuming that unicast is used for retransmissions, C_s^1 is the sum of the cost for the initial multicast from the source to all MAs (T) and the cost for retransmissions from the source to all MAs ($(E_L - 1) \cdot 2L \cdot N_{MA}$), divided by the multicast group size (M). The cost for the initial multicast equals T because each MA on the tree transmits the packet once to each of its downstream nodes [39]. The cost for retransmissions is $(E_L - 1) \cdot 2L \cdot N_{MA}$ to account for transmitting both the acknowledgements and retransmitted data packet along the paths between the source and the MAs. Therefore, C_s^1 is calculated as follows:

$$C_s^1 = \frac{1}{M}[T + (E_L - 1) \cdot 2L \cdot N_{MA}] \tag{12}$$

C_s^2 is given by the distance-probability-weighted costs for the transmissions/retransmissions from an MA to a group member, as follows:

$$C_s^2 = \sum_{h=0}^{h=H-1} P_h \cdot h \cdot E_h \tag{13}$$

The cost for mobility management (C_m) depends on the transition event in the SPN model, i.e., *Join*, *Reset*, or *MC2MA*, triggered by the movement of a member. More specifically, C_m is given by:

$$C_m = \begin{cases} 2H + (1 + P_1^{MA}) \cdot 2L & if\ Join \\ 2h + P_1^{MA} \cdot 2L & if\ Reset \\ 2h & if\ MC2MA \end{cases} \tag{14}$$

where $h = mark(Hops)$ represents the distance between the member and its MA. When the *Join* event is triggered, the cost incurred includes three components: 1) the signaling cost for deassociation from the member's current MA, 2) the signaling cost for the new MA to join the backbone multicast tree, and 3) the signaling cost for the current MA to be removed from the backbone multicast tree if it no longer services any group members. When the *Reset* event is triggered, the cost incurred includes the signaling cost for deassociation from the member's current MA and the signaling cost for the MA to be removed from the backbone multicast tree if it no longer services any group members. Finally, the signaling cost incurred when the *MC2MA* event is triggered is for the MC to report a serving MR change to its MA, which is h hops away from the MC's current serving MR.

The cost for security key management includes the cost for updating the group key K_g when an MA joins or leaves the backbone multicast tree (C_{Kg}), and the cost for a member to generate a new key K_u when it associates with a new MA (C_{Ku}). C_{Kg} is further divided into two parts, namely C_{Kg}^j and C_{Kg}^l, for MA join and leave events, respectively. C_{Kg}^j is for the source to send the updated group key to the newly joining MA (existing MAs update the group key using a one-way hash function). C_{Kg}^l is for the source to send the updated group key to the MAs excluding the one that left. C_{Kg}^j and C_{Kg}^l are therefore calculated as:

$$\begin{aligned} C_{Kg}^j &= 2L \\ C_{Kg}^l &= (N_{MA} - 1) \cdot 2L \end{aligned} \tag{15}$$

C_{Ku} is the cost for a member to execute the DH protocol to generate a new key K_u when it changes its MA. Specific to the SPN model, C_{Ku} is incurred when transition *Join* or *Reset* is fired. The execution of the protocol involves a round-trip message exchange between the member and its new MA. Therefore C_{Ku} is calculated as:

$$C_{Ku} = 2 \quad if\ Join\ or\ Reset \tag{16}$$

The cost for group membership management consists of the cost for processing a member join event (C_j) and that for processing a member leave event (C_l). When a member joins the multicast group, the new serving MR of the member may need to be subscribed to the backbone multicast tree if it is not already an MA, the probability of which is $1 - P_{MA}$. In a member leave event, the leaving member notifies its MA that is h hops away by a leave request, and if the MA no longer services any group member after the member leaves, it needs to be removed from the backbone multicast tree by forwarding the leave request to the source. Thus, C_j and C_l are calculated as:

$$\begin{array}{l} C_j = (1 - P_{MA}) \cdot 2L \\ C_l = 2h + P_1^{MA} \cdot 2L \end{array} \tag{17}$$

where $h = mark(Hops)$ represents the distance between the member and its MA.

C_{HASRM} is the sum of each cost multiplied with the rate at which the associated operation occurs, i.e., C_{HASRM} is given by:

$$\begin{array}{l} C_{HASRM} = \lambda_p \cdot C_s + \sigma \cdot (C_m + C_{Kg}^j + C_{Ku}) \\ +\lambda \cdot C_j + \mu \cdot (C_{Kg}^l + C_l) \end{array} \tag{18}$$

6 Performance Evaluation

Table 4: Parameters and their typical values.

Parameter	Meaning	Typical value
M	multicast group size	[10, 320]
n	network size	[5, 15]
λ_p	multicast packet rate	10
σ	mobility rate	$\frac{1}{600}$
λ	multicast group member join rate	$\frac{1}{30}$
μ	multicast group member leave rate	$\frac{1}{30}$
SMR	Service to mobility rate	[8, 6000]
p	loss probability of wireless links	[0.0, 0.3]

In this section, we evaluate the performance of HASRM and examine the effect of various parameters on its performance. To evaluate the effect of

user mobility on the performance of the three algorithms, we introduce a parameter called *service to mobility ratio* (SMR) defined as $SMR = \frac{\lambda_p}{\sigma}$. The physical meaning of SMR is the average number of multicast data packets transmitted from the source to a group member during the interval between two serving MR changes of the group member. The time unit used in this paper is second. For example, if on average a group member changes its serving MR once every 10 minutes and the multicast packet rate is 10 (per second), its SMR is 6000. SMR is an important parameter because it captures the service and mobility characteristics of group members, both of which can have a significant impact on the operations of HASRM and on the overall network cost.

Table 4 lists the parameters and their values used in performance evaluation. These values are selected to demonstrate diversely sized multicast groups consisting of mobile members characterized by a broad range of SMR. The member join and leave rates are chosen to allow dynamically changing group membership, while maintaining a stable multicast group size. The range of n is selected to model a WMN of reasonably diverse sizes.

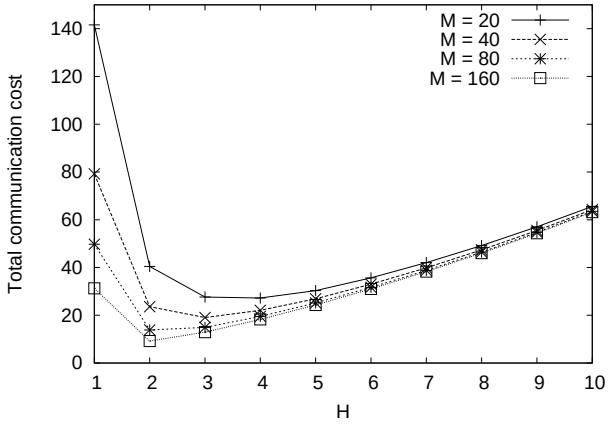

Figure 5: Cost vs. H, under different multicast group sizes in HASRM ($n = 10$).

Fig. 5 and Fig. 6 plot C_{HASRM} as a function of the threshold H, under different multicast group sizes and network sizes, respectively. As the figures show, there exists an optimal threshold $H_{optimal}$ that minimizes C_{HASRM} for each different M and n. These results demonstrate that the regional service size of an MA is key to the performance of HASRM, and there exists an op-

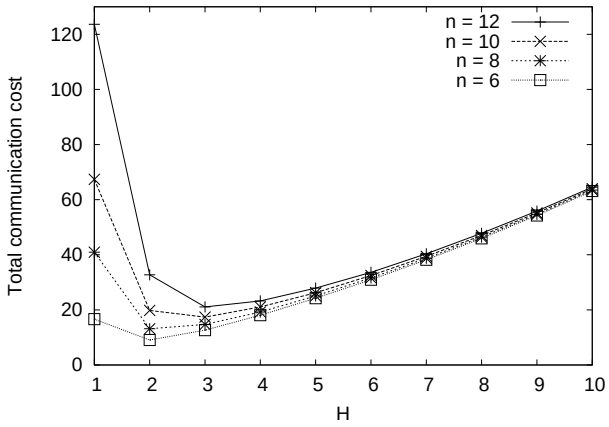

Figure 6: Cost vs. H, under different network sizes in HASRM ($M = 50$).

timal regional service size that minimizes C_{HASRM}. It can also be observed that C_{HASRM} decreases with increasing M in Fig. 5, and that C_{HASRM} decreases with decreasing n in Fig. 6. These trends suggest that the multicast member population density, defined as $\gamma = \frac{M}{n^2}$, has a significant impact on the performance of HASRM, as illustrated in Fig. 7.

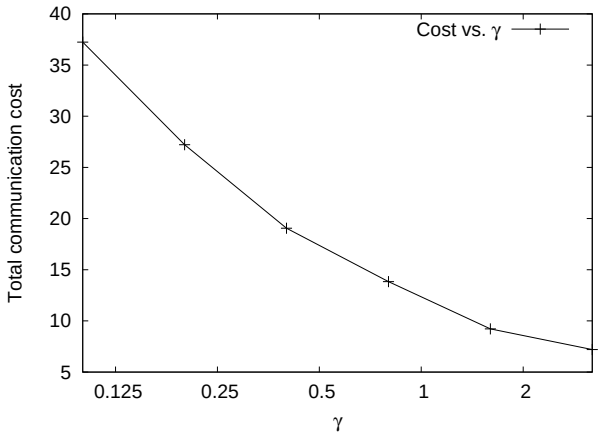

Figure 7: Cost vs. γ in HASRM.

Fig. 7 shows C_{HASRM} as a function of the multicast member population density γ. As can be seen in the figure, C_{HASRM} decreases as γ increases. This illustrates that multicast efficiency improves as the member population

density increases because the cost is effectively amortized by the increasing member population.

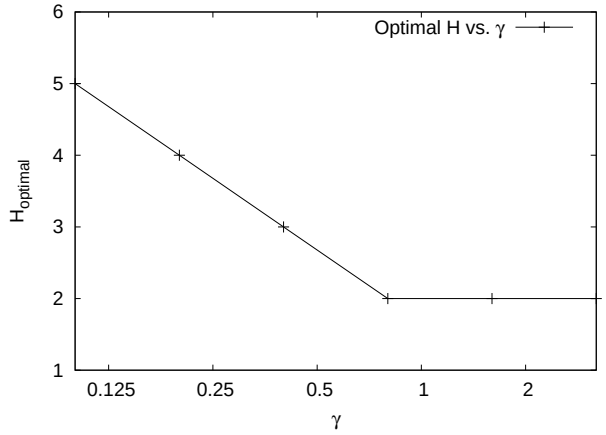

Figure 8: $H_{optimal}$ vs. γ in HASRM.

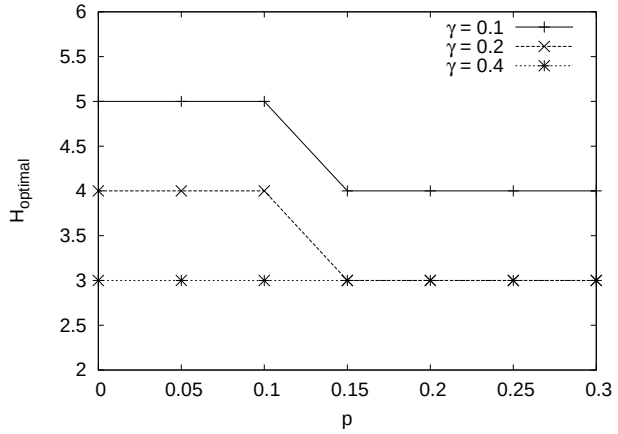

Figure 9: $H_{optimal}$ vs. p in HASRM.

Fig. 8 illustrates $H_{optimal}$ as a function of γ. We observe that $H_{optimal}$ decreases as γ increases, and drops to 1 when γ is reasonably large. Decreasing $H_{optimal}$ as γ increases keeps C_{HASRM} minimized. This is because as γ increases, the cost incurred at the lower level of the multicast hierarchy will be dominating but its magnitude will reduce with decreasing $H_{optimal}$, thereby lowering C_{HASRM}. Fig. 8 demonstrates that HASRM can adapt to

changes in member population density by dynamically determining $H_{optimal}$ that minimizes the total communication cost.

Fig. 9 plots $H_{optimal}$ as a function of p, the loss probability of wireless links, under different member population densities. As can be seen in the figure, the general trend is that $H_{optimal}$ decreases with increasing values of p. As p increases, the service cost C_s for multicast data delivery increases. Therefore, shorter paths for multicast data delivery are necessary to keep the total communication cost minimized, favoring smaller values of $H_{optimal}$ accordingly. This demonstrates one of the benefits of dynamically determining $H_{optimal}$ that minimizes C_{HASRM}, i.e., HASRM is dynamically adaptive to the quality of wireless links that may vary over time.

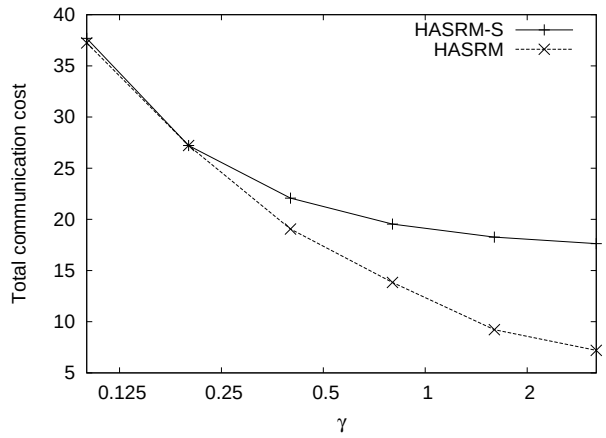

Figure 10: HASRM vs. HASRM-S as a function of γ.

To further reveal the benefit of dynamically determining $H_{optimal}$ that minimizes C_{HASRM}, we compare HASRM with a special case of HASRM that uses static MAs with a fixed threshold H, say, $H = 4$, and we name this special case HASRM-S. HASRM-S represents an extension to a class of hierarchical reliable multicast algorithms that use statically placed proxies with fixed regional service sizes for decentralized management. Specifically, the extension is for mobility and security support. Fig. 10 compares the total communication costs incurred by HASRM and HASRM-S respectively as a function of γ. As the figure shows, HASRM significantly outperforms HASRM-S, especially when γ becomes large.

Fig. 11 investigates the effect of SMR on the performance of HASRM and HASRM-S. We observe that HASRM significantly performs better than

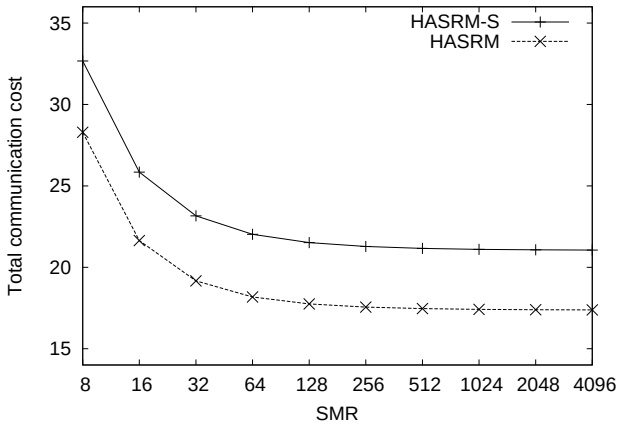

Figure 11: HASRM vs. HASRM-S as a function of SMR.

HASRM-S over a wide range of SMR values representing diverse user mobility and multicast service characteristics. HASRM outperforms HASRM-S in both cases because it can adapt to the changing member population density and movement frequency by dynamically determining the optimal MA regional service size ($H_{optimal}$) that keeps the total communication cost minimized.

7 Comparative Performance Study

We compare HASRM with traditional multicast algorithms based on a shortest-path tree (SPT) [40] extended with user mobility, security, and reliability support (named the SPT algorithm). The SPT algorithm maintains an SPT rooted at the source with multicast group members as tree leaves for multicast data delivery. The multicast tree in the SPT algorithm is updated to maintain its structural properties every time a member moves and changes its serving MR. A group key K_g is used for secure multicast data delivery from the source to the group members. Whenever a group member joins or leaves, the group key K_g needs to be updated for all group members to ensure the forward and backward secrecy properties. NAK-based retransmissions are used to provide reliable multicast data delivery.

Fig. 12 compares the total communication cost incurred as a function of γ, between HASRM and SPT. As expected, for both algorithms, the total

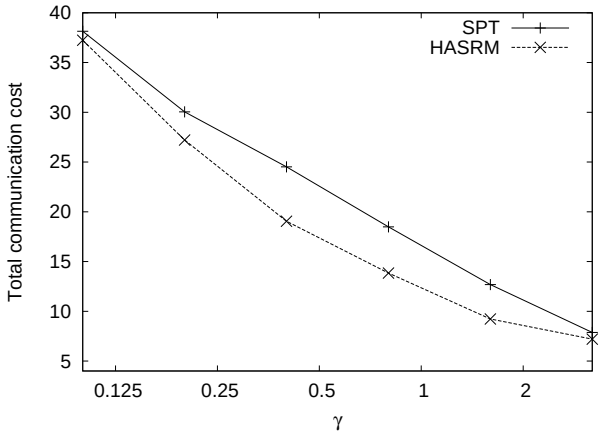

Figure 12: HASRM vs. SPT as a function of γ.

communication cost decreases with increasing γ, because multicast efficiency improves as the member population density increases. As can be seen in the figure, HASRM is superior to SPT, particularly for moderate values of γ. It is worth emphasizing that because the total communication cost is a per member per time unit metric, even a small cost reduction of 5% to 10% will be significant over time and over the entire group of members.

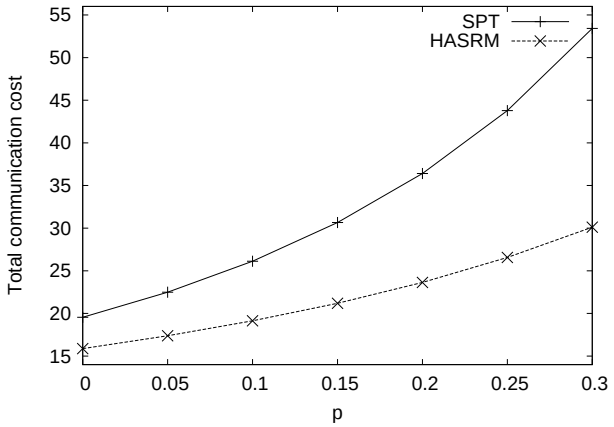

Figure 13: HASRM vs. SPT as a function of p.

Fig. 13 compares the total communication cost incurred as a function of p, the loss probability of wireless links, between HASRM and SPT. As expected,

the total communication cost increases with increasing p for both algorithms, because the service cost for reliable multicast data delivery increases as p increases. Again, HASRM performs significantly and consistently better than SPT. More importantly, it can be seen that HASRM copes much better than SPT with changing quality of wireless links.

We also perform a comparative performance study between HASRM and a recently proposed protocol framework for secure group communications in WMNs, called Secure Group Overlay Multicast (SeGrOM) [2]. SeGrOM is also a hierarchical decentralized multicast algorithm, and it handles member mobility and dynamic group membership with decentralized management. SeGrOM uses a two-tier multicast structure and two sub-protocols for multicast data delivery in the two tiers. The global data delivery protocol transmits multicast data via a secure overlay to head members, which are elected coordinators for local data delivery and group membership management. There is one coordinator for each subgroup of group members connected to the same MR. Whenever an coordinator leaves the MR to which it is connected, a new coordinator needs to be elected and subscribed to the secure overlay. If a member joins the multicast group via an MR without existing members, the member becomes a new coordinator and joins the secure overlay. The coordinator maintains a local data key shared among all members associated with the same MR for encrypting multicast packets. The local data key is refreshed (rekeyed) whenever a member associated with the same MR joins or leaves.

It can be seen that coordinators are similar to MAs except that coordinators are group members that are dynamic. Indeed, because each coordinator is always associated with an MR, the secure overlay in SeGrOM can be considered as consisting of a dynamic group of MRs. A difference is that the regional service size of an MA is dynamically determined by HASRM, whereas the service area of a coordinator is exactly the coverage area of an MR. To make the comparison between HASRM and SeGrOM on a fair basis, we will use a variant of HASRM that does not address reliability. For similar reason, we compare the variant of HASRM with a variant of SeGrOM called SeGrOM-Group because like HASRM, this variant also uses a group key for data encryption and the secure overlay for group key distribution. It is worth noticing that SeGrOM does not address general mobility management, i.e., it does not consider mobility management as a general service that is necessary not only for mobile multicast, but also for other network services.

Fig. 14 compares the total communication cost incurred as a function of

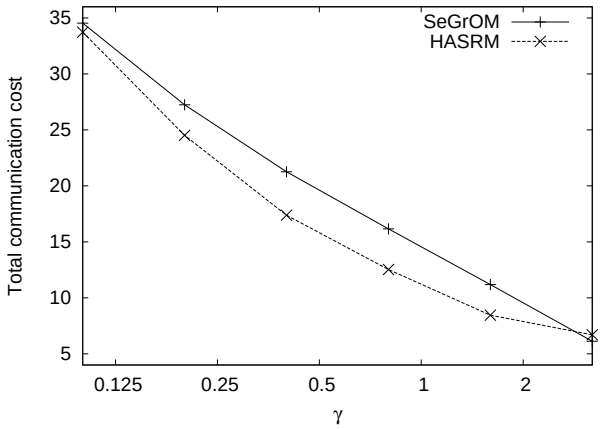

Figure 14: HASRM vs. SeGrOM as a function of γ.

γ, between HASRM and SeGrOM. As can be seen in the figure, HASRM outperforms SeGrOM for a wide range of values of γ. SeGrOM is slightly better only when γ is considerably large. Note that the total communication cost incurred by HASRM also includes the signaling cost for mobility management, making HASRM applicable to any network services. It is worth emphasizing again that because the total communication cost is a per member per time unit metric, even a small cost reduction of 5% to 10% will be significant over time and over the entire group of members.

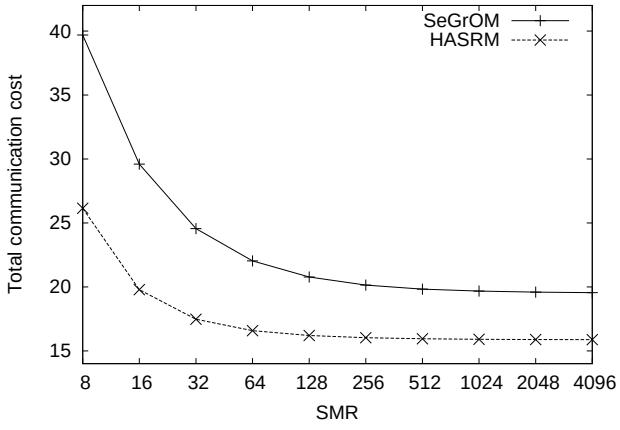

Figure 15: HASRM vs. SeGrOM as a function of SMR.

Fig. 15 further compares between HASRM and SeGrOM the total communication cost incurred as a function of SMR. As the figure shows, HASRM performs consistently better than SeGrOM for the investigated range of SMR, particularly when SMR is small, i.e., when the mobility rate is high. It shows that HASRM copes well with high group member mobility and is adaptive to the varying mobility rate. This is attributive to the design principle of integrated mobility and service management.

8 Simulation Validation

In this section, we conduct discrete-event simulations using a simulation language Simulation Model Programming Language (SMPL) [41] to validate the results obtained through the analytical model. To ensure the statistical significance of simulation results, we use a batch mean analysis technique. Each simulation batch consists of a large number of runs and therefore a large number of observations for computing one batch average. The simulation runs for a minimum of 10 batches, and stops until the mean of the batch means collected is within 5% from the true mean with a confidence level of 95%. In the simulation study we use the same set of parameter values as those listed in Table 4.

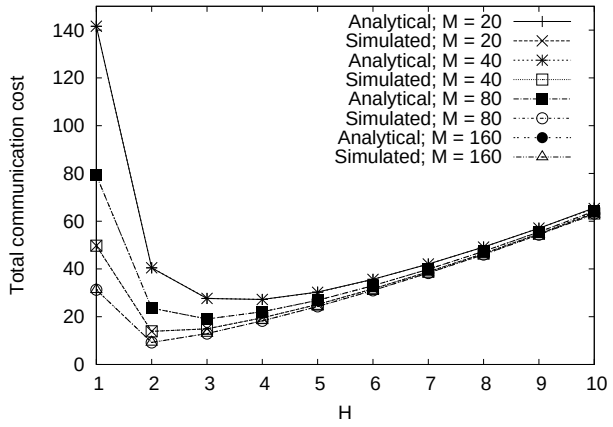

Figure 16: Simulated cost vs. H, under different multicast group sizes in HASRM ($n = 10$).

Fig. 16 compares the analytical results vs. the simulation results for

C_{HASRM} as a function of H under different multicast group sizes. The figure shows a perfect correlation between the analytical results and simulation results. Similarly, A perfect correlation between the analytical results and simulation results can be observed in Fig. 17, which compares the analytical results vs. the simulation results for C_{HASRM} as a function of γ.

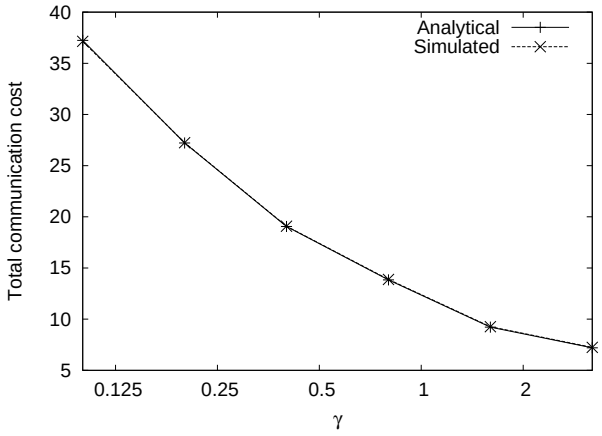

Figure 17: Simulated cost vs. γ in HASRM.

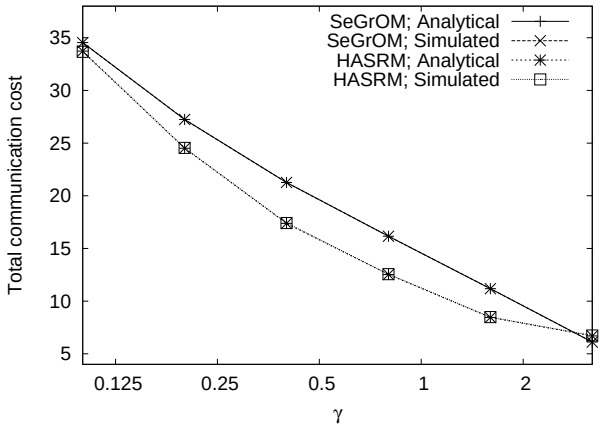

Figure 18: Simulated HASRM vs. SeGrOM as a function of γ.

Fig. 18 compares the simulation results against the analytical results shown in Fig. 14. Again, the simulation results are perfectly correlated with

the analytical results. These results demonstrate that the analytical model is valid and it accurately captures the operation of HASRM.

9 Practicability and Implementation

We discuss in this section practical issues related to the implementation of HASRM on real mobile devices that can be highly diverse with respect to their computing power and storage capacity. One important issue is how to dynamically determine $H_{optimal}$ at runtime. For powerful mobile devices that are equipped with state-of-the-art processors, the computational procedure developed in this paper can be easily executed to determine $H_{optimal}$ at runtime on a periodic basis. For mobile devices that are less powerful, a simple table-lookup approach can be used to determine $H_{optimal}$ at runtime. Specifically, the values of $H_{optimal}$ can be calculated at static time for wide ranges of system parameters and stored in a table for fast lookup. At runtime, $H_{optimal}$ can be easily determined by looking up in the table using the estimated values of those parameters as keys. Overall, the implementation can be lightweight and very efficient.

To execute the computational procedure presented in the paper, a mobile device needs to first collect data for estimating the values of parameters such as the mobility rate (σ), the multicast packet rate (λ_p), the rates of member join/leave events (λ and μ), and the loss probability of wireless links (p). σ can be estimated periodically by an MC by counting the number of serving MR changes during a fixed interval, say, every 30 minutes. A serving MR change can be detected by a change in the ID number of the current serving MR. Specifically, the MC maintains a counter for the number of serving MR changes, and the counter is incremented whenever the MC changes its serving MR. At the end of each interval, the mobility rate is calculated and the counter is reset. Similarly, the MC can dynamically estimate λ_p and p by monitoring the sequence numbers of received multicast packets. λ and μ can be monitored dynamically by the source and periodically distributed to the group members.

10 Conclusions and Future Work

In this paper, we proposed a hierarchical agent-based secure and reliable multicast (HASRM) algorithm for efficiently supporting secure and reliable mobile multicast in wireless mesh networks. HASRM minimizes the overall communication cost incurred collectively by reliable multicast packet delivery, mobility management, security key management, and group membership management. HASRM achieves cost minimization by dynamically maintaining a group of MAs for integrated mobility and multicast service management and dynamically determining optimal regional service sizes of MAs as identified in the paper, when given a set of parameter values characterizing the networking environment, as well as the user mobility and multicast service behaviors. We demonstrated via a comparative performance study that HASRM significantly outperforms traditional algorithms based on shortest-path multicast trees extended with user mobility, security, and reliability support. We also showed that a variant of HASRM is superior to a recently proposed algorithm for secure group communications in WMNs.

In the future, we plan to extend HASRM to handle failures of MRs and MAs in addition to packet losses on wireless links such that it offers a more complete solution to secure and reliable multicast in WMNs. We also plan to study methods for efficiently supporting source mobility. Another direction to explore is to use MCs alternatively to MRs as MAs when some group members cannot find a nearby MR and must rely on other MCs for network traffic relaying. Having MCs serve as MAs extends the coverage area of a multicast group to those members that are not connected to an MR.

References

[1] I.F. Akyildiz, X. Wang, W. Wang, Wireless mesh networks: a survey, Computer Networks 47 (4) (2005) pp. 445–487.

[2] J. Dong, K. Ackermann, C. Nita-Rotaru, Secure group communication in wireless mesh networks, Ad Hoc Networks 7 (8) (2009) pp. 1563–1576.

[3] S. Mittra, Iolus: a framework for scalable secure multicasting, ACM SIGCOMM, 1997, pp. 277–288.

[4] Y. Li, I.R. Chen, Design and performance analysis of mobility management schemes based on pointer forwarding for wireless mesh networks, IEEE Transactions on Mobile Computing, 10 (3) (2011), pp. 349-361.

[5] Y. Li, I.R. Chen, Mobility management in wireless mesh networks utilizing location routing and pointer forwarding, IEEE Transactions on Network and Service Management 9 (3) (2012), pp. 226-239.

[6] B. Gu, I.R. Chen, Performance analysis of location-aware mobile service proxies for reducing network cost in personal communication systems, Mobile Networks and Applications 10 (4) (2005), pp. 453-463.

[7] I.R. Chen, T.M. Chen, C. Lee, Performance evaluation of forwarding strategies for location management in mobile networks, The Computer Journal 41 (4) (1998), pp. 243-253.

[8] I.R. Chen, T.M. Chen, C. Lee, Agent-based forwarding strategies for reducing location management cost in mobile networks, Mobile Networks and Applications 6 (2) (2001), pp. 105-115.

[9] C. Hirel, B. Tuffin, K. S. Trivedi, SPNP: Stochastic petri nets. version 6.0, Proceedings of the 11th International Conference on Computer Performance Evaluation: Modelling Techniques and Tools, London, UK TOOLS, 2000, pp. 354–357.

[10] I.R. Chen, D.C. Wang, Analyzing Dynamic Voting using Petri Nets, 15th IEEE Symposium on Reliable Distributed Systems, Niagara Falls, Canada, 1996, pp. 44–53.

[11] I.R. Chen, F. Bao, M. Chang, J.H. Cho, Trust Management for Encounter-based Routing in Delay Tolerant Networks, IEEE Global Telecommunications Conference, Miami, 2010, pp. 1-6.

[12] S.T. Cheng, C.M. Chen, I.R. Chen, Dynamic Quota-based Admission Control with Sub-rating in Multimedia Servers, Multimedia Systems 8(2) (2000) pp. 83–91.

[13] S.T. Cheng, C.M. Chen, I.R. Chen, Performance Evaluation of an Admission Control Algorithm: Dynamic Threshold with Negotiation, Performance Evaluation 52 (1) (2003) pp. 1-13.

[14] I.R. Chen, T.H. Hsi, Performance Analysis of Admission Control Algorithms based on Reward Optimization for Real-time Multimedia Servers, Performance Evaluation 33 (2) (1998) pp. 89-112.

[15] I.R. Chen, F.B. Bastani, T.W. Tsao, On the Reliability of AI Planning Software in Real-time Applications, IEEE Transactions on Knowledge and Data Engineering 7 (1) (1995) pp. 4-13.

[16] I.R. Chen, F.B. Bastani, Effect of Artificial-Intelligence Planning-Procedures on System Reliability, IEEE Transactions on Reliability 40 (3) (1991) pp. 364-369.

[17] I.R. Chen, D.C. Wang, Analysis of Replicated Data with Repair Dependency, The Computer Journal 39(9) (1996) pp. 767-779.

[18] Y. Li, I.R. Chen, Hierarchical Agent-Based Secure Multicast for Wireless Mesh Networks, IEEE International Conference on Communications, Kyoto, Japan, 2011.

[19] C. Perkins, IP Mobility Support for IPv4, IETF RFC 3344, 2002.

[20] Y. Huh, C. Kim, mMOM: Efficient Mobile Multicast Support Based on the Mobility of Mobile Hosts, Wireless Networks 12 (2) (2006) pp. 171–178.

[21] C. Liu, K. Wang, Mobile Multicast Support in IP Networks, 19th IEEE International Conference on Computer Communications, 2000, pp. 1664–1672.

[22] I.R. Chen, D.C. Wang, Regional registration-based mobile multicast service management in mobile IP networks, Wireless Personal Communications 54 (4) (2010) pp. 635–649.

[23] W. Liao, C.-A. Ke, J.-R. Lai, Reliable multicast with host mobility, IEEE Global Telecommunications Conference, 2000, pp. 1692–1696.

[24] G. Zeng, B. Wang, Y. Ding, L. Xiao, M. W. Mutka, Efficient multicast algorithms for multichannel wireless mesh networks, IEEE Transactions on Parallel and Distributed Systems 21 (1) (2010) pp. 86–99.

[25] I. Chakeres, C. Koundinya, P. Aggarwal, Fast, efficient, and robust multicast in wireless mesh networks, 5th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, 2008, pp. 19–26.

[26] J. Yuan, Z. Li, B. Li, A Cross-Layer Optimization Framework for Multihop Multicast in Wireless Mesh Networks, IEEE Journal of Selected Areas in Communications 24 (11) (2006) pp. 2092–2103.

[27] P. M. Ruiz, F. J. Galera, C. Jelger, T. Noel, Efficient multicast routing in wireless mesh networks connected to Internet, 1st International Conference on Integrated Internet Ad Hoc and Sensor Networks, 2006.

[28] Y. Sun, W. Trappe, K. J. Ray Liu, A Scalable Multicast Key Management Scheme for Heterogeneous Wireless Networks, IEEE/ACM Transactions on Networking 12 (4) (2004) pp. 653–666.

[29] S. Shin, J. Hur, H. Lee, H. Yoon, Bandwidth Efficient Key Distribution for Secure Multicast in Dynamic Wireless Mesh Networks, IEEE Wireless Communications and Networking Conference, 2009, pp. 2202–2207.

[30] A. Noack, J. Schwenk, Group key agreement for wireless mesh networks, 5th LCN Workshop on Security in Communications Networks, 2009, pp. 945–952.

[31] D. Koutsonikolas, Y. Charlie Hu, C.C. Wang, Pacifier: High-Throughput, Reliable Multicast without "Crying Babies" in Wireless Mesh Networks, 28th Annual IEEE Conference on Computer Communications, 2009, pp. 2473–2481.

[32] S. Guha, A. Markopoulou, F. Tobagi, Hierarchical reliable multicast: performance analysis and optimal placement of proxies, Computer Communications 26 (18) (2003) pp. 2070–2081.

[33] S. Paul, K. Sabnani, J. Lin, S. Bhattacharyya, Reliable multicast transport protocol (rmtp), IEEE Journal on Selected Areas in Communications 15 (3) (1997) pp. 407–421.

[34] W. Diffie, M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22 (6) (1976) pp. 644–654.

[35] A. T. Sherman, D. A. McGrew, Key Establishment in Large Dynamic Groups Using One-Way Function Trees, IEEE Transactions on Software Engineering 19 (5) (2003) pp. 444–458.

[36] C. K. Wong, M. Gouda, S. S. Lam, Secure Group Communications Using Key Graphs, IEEE/ACM Transactions on Networking 8 (1) (2000) pp. 16–30.

[37] J. C.-I. Chuang, M. A. Sirbu, Pricing multicast communication: a cost-based approach, Telecommunication Systems 17 (3) (2004) pp. 281–297.

[38] R. C. Chalmers, K. C. Almeroth, On the topology of multicast trees, IEEE/ACM Transactions on Networking 11 (1) (2003) pp. 153–165.

[39] P. M. Ruiz, A. F. Gomez-Skarmeta, Approximating optimal multicast trees in wireless multihop networks, 10th IEEE Symposium on Computers and Communications, 2005, pp. 686–691.

[40] U. T. Nguyen, On multicast routing in wireless mesh networks, Computer Communications 31 (7) (2008) pp. 1385–1399.

[41] M. H. MacDougall, Simulating Computer Systems: Techniques and Tools, MIT Press, 1987.