Secure Group Communication in Wireless Mesh Networks

Jing Dong*, Kurt Ackermann, Cristina Nita-Rotaru

Department of Computer Science, Purdue University
305 N. University St., West Lafayette, IN 47907 USA

Abstract

Wireless mesh networks (WMNs) have emerged as a promising technology that offers low-cost community wireless services. The community-oriented nature of WMNs facilitates group applications, such as webcast, distance learning, online gaming, video conferencing, and multimedia broadcasting. Security is critical for the deployment of these services. Previous work focused primarily on MAC and routing protocol security, while application-level security has received relatively little attention. In this paper we focus on providing data confidentiality for group communication in WMNs. Compared to other network environments, WMNs present new challenges and opportunities in designing such protocols. We propose a new protocol framework, *Secure Group Overlay Multicast (SeGrOM)*, that employs decentralized group membership, promotes localized communication, and leverages the wireless broadcast nature to achieve efficient and secure group communication. We analyze the performance and discuss the security properties of our protocols. We demonstrate through simulations that our protocols provide good performance and incur a significantly smaller overhead than a baseline centralized protocol optimized for WMNs.

Key words: group communication, secure group communication, group key management, wireless mesh networks

1. Introduction

Wireless mesh networks (WMNs) have emerged as a promising technology that offers low-cost high-bandwidth community wireless services. A WMN consists of a set of stationary wireless routers that form a multi-hop wireless backbone, and a set of mobile clients that communicate via the backbone routers. The community-oriented nature of WMNs facilitates group applications, such as webcast, distance learning, online gaming, video conferencing, and multimedia broadcasting. Many of these applications follow a communication pattern in which one or more source clients disseminate data to a changing set of receivers. The openness of the wireless environment makes security a critical concern in the deployment of such group applications.

A major security goal for group applications is providing data confidentiality such that only current group members have access to the data sent to the group. Previous communication must remain protected from newly joined members, and future communication must be protected from members who have left the group. Examples of applications that can benefit from these services are applications which disseminate sensitive content, such as multimedia conferencing, and applications which seek to ensure that only clients that have paid or registered for service can receive data, such as online video broadcasting and distance learning.

WMNs present unique features that pose new challenges in designing secure group communication protocols. In WMNs, the backbone routers and wireless clients form a unique two-tier architecture, with distinct mobility and power constraints. Backbone routers communicate via multi-hop wireless links, which have

*Corresponding author. Phone: 1-765-496-9398 Fax: 1-765-494-0739
Email addresses: dongj@cs.purdue.edu (Jing Dong), keackerm@cs.purdue.edu (Kurt Ackermann), crisn@cs.purdue.edu (Cristina Nita-Rotaru)

high loss rate and latency. WMNs also present new opportunities for designing more efficient secure group communication protocols than the ones proposed for wired or mobile ad hoc networks (MANETs). The wireless broadcast can be leveraged to reduce bandwidth consumption. Static routers provide a decentralized and more stable structure than MANETs. Multiple clients sharing the same access router can also be used for a more localized communication. Finally, unlike MANETs, mobile clients often exhibit only localized mobility in WMNs [1].

Existing solutions for wired networks [2, 3, 4, 5, 6] are not well suited for WMNs as they assume efficient reliable end-to-end and multicast delivery, which is much more expensive to achieve in a multi-hop wireless environment. These protocols also do not exploit unique features of WMNs, such as the broadcast nature of wireless communication. Solutions proposed for wireless sensor networks (WSNs) [7], [8], [9] and MANETs [10], [11], [12] are designed to sustain severe computation power, storage, mobility, and energy constraints, and as a result have limited scalability and robustness.

In this paper, we focus on the problem of ensuring data confidentiality for group communications in WMNs, considering their unique challenges and opportunities. The main contributions of this paper are:

- We propose a new protocol framework for secure group communication, *Secure Group Overlay Multicast (SeGrOM)*, that employs decentralized group membership, promotes localized communication, and leverages the wireless broadcast nature to efficiently accommodate dynamic group changes and reduce communication overhead. We present three secure multicast variants supported by our framework, with different trade-offs in complexity, cost, and security, and an efficient group revocation protocol that exploits localized client mobility.

- We demonstrate analytically the significant reduction of bandwidth overhead (up to 10 times) and latency (up to 80 times) of the proposed protocols over a centralized scheme that is optimized for wireless networks.

- We validate our protocols experimentally with extensive simulations based on the *ns2* simulator [13]. Simulation results show that all of the proposed protocols provide good performance (comparable with the unprotected communication protocol) and incur a significantly smaller overhead than our baseline centralized protocol that is optimized for wireless networks. Our protocols reduce the bandwidth overhead and latency by about 85% when handling group changes.

Roadmap: We present related work in Section 2. The network and security model and the design goals are described in Section 3. Section 4 describes the SeGrOM protocols. The performance analysis is presented in Sections 5. The experimental results are presented in Sections 6. Finally, Section 7 concludes the paper.

2. Related Work

Secure group communication is a mature research area and has a large body of research literature. The main objective of a secure group communication protocol is to ensure the data confidentiality against outsiders such that only legitimate group members can recover the group data. In the following, we give a brief overview of existing work in this area in both traditional wired networks and wireless networks, respectively.

Secure Group Communication in Wired Networks. A general approach to secure group communication is to use a group key shared among group members to encrypt group data. Depending on the specific *group key management* protocol used, we can classify existing schemes into group key distribution schemes and contributory group key agreement schemes.

In a group key distribution scheme, a centralized entity (e.g. the data source or the group manager) generates the group key and distributes the key to all the group members. The most well-known protocols in this category are the tree-based key management protocols like LKH [2] and its variants [14, 15, 16, 17, 18]. These protocols maintain global membership and require direct communication to the source node for both group joins and leaves. Reliable key delivery is achieved with redundant packets (forward error correction)

and end-to-end unicast recovery. The high bandwidth and latency overhead of such protocols make them unsuitable for the multi-hop wireless environment.

Another direction of group key distribution is the hierarchical group key management schemes like Iolus [19]. Iolus explicitly constructs sub-groups based on trusted *group security agents* (GSAs) and achieves scalability by handling group dynamics within each sub-group. Our proposed framework, SeGrOM, shares the same spirit as Iolus in that it also localizes the handling of group dynamics. But unlike Iolus, SeGrOM localizes the traffic to the router level, which matches the unique two-tier architecture of WMNs, to achieve a much more fine-grained traffic localization. In addition, SeGrOM does not require trusted GSAs deployed in the network. Finally, SeGrOM, being designed specifically for wireless networks, also encompasses mechanisms for leveraging the broadcast advantage of wireless transmission for improved efficiency.

In contributory key agreement schemes, the group key is generated from uniform contributions from all group members by using schemes such as n-party Diffie-Hellman key exchange. In general, these schemes [20, 21, 22] require reliable communication from each group member to every other group member on handling group dynamics. Such reliable broadcast communication is extremely inefficient to achieve in multi-hop wireless networks, rendering them not suitable for WMNs.

Recent work on secure group communication in wired networks has also focused on the specific environment of overlay multicast networks [23, 24, 25, 6]. Although overlay networks are also multi-hop in nature, they do not have the properties of client mobility, multiple clients sharing the same access router, or the much more limited bandwidth resource as in WMNs. As a result, the protocols built for overlay networks are also not well-suited for WMNs.

Secure Group Communication in Wireless Networks. Due to the constrained resource in the wireless environment, the basic approach to secure group communication in wireless networks is to match the protocol structure with the structure of wireless networks in order to achieve improved performance and efficiency. Below we briefly discuss existing protocols proposed for cellular networks and mobile ad hoc networks (MANETs).

Cellular networks also exhibit a two-tier architecture, with high-bandwidth wired links connecting base stations (BSs) and low-bandwidth links between BS and clients. The work in [26] proposes a topology matching key management (TMKM) scheme that adapts the traditional key tree (LKH) to match the two level structure of cellular networks. TMKM does not consider the problem of key distribution among BSs, as they are connected with high-bandwidth wired links. However, in WMNs, mesh routers are connected with multi-hop wireless links, thus it is crucial to also consider the communication on the backbone routers in designing a secure group communication protocol.

The work in secure group communication in MANETs include GKMPAN [10], CRTDH [11] and the work in [12]. GKMPAN is a group key management scheme designed for a relatively stable group, and focuses primarily on member revocation. The scheme uses pair-wise keys to distribute a common group key for data encryption among group members. CRTDH [11] relies on the Chinese Remainder Theorem and the Diffie-Hellman group key agreement for establishing group keys. It requires a number of messages linear to the group size to refresh the key for every group join and leave. Thus, it is not scalable in a wireless environment with limited bandwidth resource. Kaya et al [12] adopts a distributed scheme for handling group dynamics to address the high overhead of multi-hop communication in MANETs. However, the scheme fails to exploit the broadcast advantage of wireless communication, primarily due to the highly dynamic nature of MANETs which prevents the establishment of a local sub-group key for data delivery.

In general, none of the existing protocols considered the unique features of WMNs, such as static backbone routers and multiple clients sharing the same router, all of which can be leveraged for designing more optimized protocols. Our work tries to fill this gap by designing such a scheme specifically for WMNs.

A relevant area of work to secure group communication is securing the underlying multicast protocols, such as [27, 28]. These schemes primarily focus on the denial-of-service attacks against the data forwarding process, thus they are complementary to the problem of achieving data confidentiality that we focus on. Another relevant research area is key pre-distribution schemes for wireless sensor networks [7], [8], [9]. These schemes focus on secure pair-wise communication, instead of group communication. Finally, a necessary condition to secure group communications is the ability to authenticate users. The protocols in [29, 30]

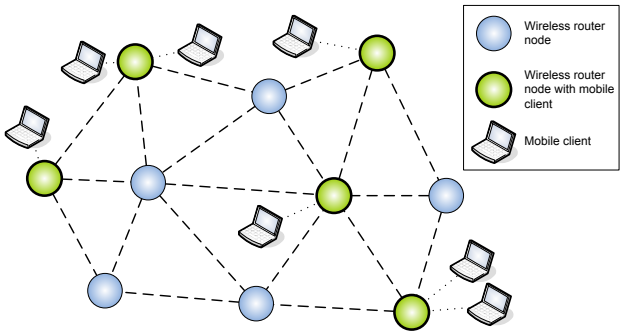


Figure 1: Example mesh network

present efficient mesh client authentication schemes on WMNs. These schemes can be used in conjunction with SeGrOM for authenticating group members in the secure group communications.

3. System Model and Design Goals

Network Model. Our target network environment is WMNs, consisting of a set of static wireless routers organized in a backbone network and communicating through multi-hop wireless links. Mobile clients connect to the wireless mesh through a local *access router* and communicate with each other through the wireless mesh (See Fig. 1). Both clients and routers can fail.

We assume that the wireless channel is symmetric; all nodes have the same transmitting power and consequently the same transmission range. We assume that group communication support is available through a tree-based on-demand multicast protocol. For concreteness, we consider the well-known MAODV [31] multicast protocol in presenting our protocols.

During a group communication session, the group members can join or leave the group at any time, with potentially high membership dynamics, possibly due to client movement or flash crowd phenomenon [32].

Security Assumptions. We assume that each client authorized to be part of the mesh network has a pair of public/private keys and a *client certificate* that binds its public key to a unique user identifier. A group manager, acting as a certificate authority (CA), is responsible for authorizing clients to join the group by issuing them a *member certificate*. This member certificate binds the client certificate to the multicast group identifier, e.g. group IP address, and serves as proof of the client's membership. We assume all group members know the public key of the group manager, so that all member certificates can be verified by any group member.

Security Goals and Adversarial Model. Our focus is on providing data confidentiality from outside adversaries (both passive and active), where an outsider is any non-group member client or backbone router. More specifically, the goal is to provide the *group secrecy* property, such that it is computationally infeasible for a non-member node (mobile client or backbone router) to discover the group data. This also includes the *backward* and *forward secrecy* properties which guarantee that it is computationally infeasible for a member client to gain access to the group data sent before the time it joins the group, or after the time it leaves (or is revoked from) the group, respectively.

We assume that current group members do not leak data or keys to routers or unauthorized clients. As authorized members may leak data via out-of-band channels, preventing such data leakage is outside the scope of our work. We do not consider attacks against the multicast protocol itself. For example, we do not consider denial of service attacks against data forwarding, and assume routers forward application and control data according to protocol specifications. Protecting the multicast protocol, e.g. [27, 28], is complementary to our work.

s	the source node
r	any group member (receiver)
h_i	the header member of the access router associated with member i
a_i	the access router associated with member i
m	the group data packet
m_e	the encrypted group data packet

Table 1: Notations used in Algorithms 1, 2, 3 and 4.

Algorithm 1: Flow of data packet m from source node s to group members.

Input: Packet m to be sent
1 s sends m to its local head member h_s;
2 h_s sends m to local receivers via the local_protocol at a_s;
3 h_s forwards m to h_r via the global_protocol;
`// Code executed by any head member` h_r
4 h_r sends m to its local receivers via the local_protocol at a_r;
5 h_r forwards m to other h'_r via the global_protocol;

4. SeGrOM Framework and Protocols

In this section, we introduce SeGrOM, our protocol framework for secure group communication in WMNs. We provide an overview of the framework, describe three protocol variants with different trade-offs in complexity, performance and security, and present an efficient member revocation mechanism. For clarity, we assume a single source multicast case in the description, however, the protocol can be easily extended to a multi-source scenario.

4.1. Overview

SeGrOM is designed to address the specific characteristics of WMNs, reducing communication overhead and latency while maintaining group data confidentiality. SeGrOM handles member mobility and group dynamics with decentralized membership management, thus avoiding the cost of multi-hop communication and obtaining lower bandwidth overhead and latency. To achieve the decentralized membership management, as well as to exploit the two-tier architecture of WMNs and the wireless broadcast nature, SeGrOM uses a hierarchical architecture consisting of two sub-protocols, a *global data delivery protocol* for inter-router backbone communication and a *local data delivery protocol* for efficient group data delivery to members connected to the same access router. The global data delivery is achieved via a secure overlay established on top of the wireless multicast protocol running on the backbone routers. SeGrOM supports three different variants for the global data delivery protocol, trading complexity, security and communication cost.

The local delivery protocol runs among members connected to the same access router, with one member client elected as the coordinator, referred to as the *head member*. The head member of an access router allows joins and leaves to be handled locally. It also coordinates the secure local data delivery and participates in the global delivery protocol on behalf of all the members connected to that access router.

Finally, SeGrOM encompasses an efficient revocation protocol which takes advantage of the localized mobility of clients. For convenience of description, we will use the notations as defined in Table 1 in describing the protocols.

The flow of a group data packet m is presented in Algorithm 1. The source s first securely forwards the packet to its local head member h_s, which delivers m to other members connected to the same access router via the local data delivery protocol, and then disperses m to all other head members via the global data delivery protocol. Each head member h_r, on receiving the packet, forwards it to the group members on the same access router a_r via the local data delivery protocol and to other head members h'_r via the global delivery protocol.

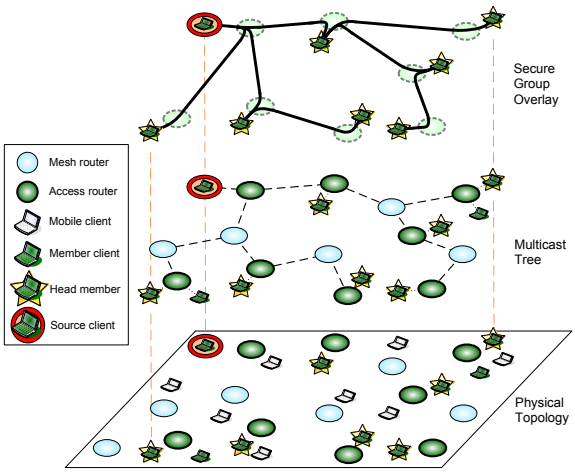


Figure 2: Conceptual abstraction of the secure group overlay

4.2. Secure Local Data Delivery

The secure local delivery of group data within a router is coordinated by the head member of that router. Each head member maintains a *local data key*, which is shared among all member clients associated with the same router. When receiving a group data packet, the head member encrypts the data packet with the local data key and forwards it to the access router, which then broadcasts the encrypted packet to all other member clients associated with the router.

Head members handle joins and leaves as follows. When a new client joins the group, it sends the join request to the local head member. After verifying the *member certificate*, the local head member refreshes the *local data key* and sends the new key to the joining node allowing it to receive the group data. The verification of the *member certificate* ensures that only authorized clients can join the group. When a client leaves the group, either gracefully by informing the head member or by crashing, the head member refreshes the *local data key* and distributes it only to the remaining member clients.

The refreshment of the local data key upon any group join and leave ensures the forward and backward secrecy of data. Due to the small scale and local communication, local data key refreshment can be achieved by encrypting the new *local data key* for each of the local member clients using pair-wise or public keys.

When a member client joins the group via a router with no existing member clients, the new member client becomes the head member for the router. When the head member for a router leaves, a new head member is elected among the remaining local member clients. Since we do not impose any additional security assumptions on head members, each member client in a router is equally eligible to be the head member, and a simple leader election algorithm, such as electing the node with the minimum identifier, can be used. The traffic for electing the head member is restricted to only the member clients in the local router.

4.3. Secure Group Overlay

For secure global data delivery, the framework maintains a secure group overlay among all the head members, on top of the underlying backbone multicast tree (See Fig. 2). Two head members are connected by a link on the overlay if on the underlying multicast tree there is no other router with active member clients between them. We refer to head members connected by a link in the overlay as *adjacent head members*. Each head member maintains a list of its adjacent head members, and establishes and discards symmetric keys (or *link keys*) upon the join and leave of their adjacent head members. A link key is established using standard authenticated key exchange protocols such as Diffie-Hellman [33]. Since multicast protocols typically keep track of neighboring nodes, the list of adjacent head members is typically readily available information.

The secure overlay is updated only when the head members change, i.e. a head member at some access router left, or a member joins the group via a router with no existing members, thus becoming the new head

Algorithm 2: Global data delivery with SeGrOM-Group.

Input: Packet m to be sent from h_s to any h_r

1 h_s encrypts m with group key K_g, result is m_e;
2 h_s sends m_e to h_r via MAODV;
3 h_r decrypts m_e with group key K_g, result is m;

member. The join/leave of head members is handled by the head member of the upstream router on the multicast tree. Under normal operation when the head members do not change, the join and leave of other members are handled locally by their local head member as described in Section 4.2.

4.4. Global Data Delivery on the Secure Overlay

The global data delivery protocol uses the secure overlay to disseminate data among head members. We consider two approaches. In the first approach, SeGrOM-Group, the head members share a common group key to encrypt the data. The group key is distributed and periodically refreshed using the secure overlay. In the second approach, SeGrOM-Link, instead of maintaining a group key, data is encrypted using a per-packet key selected by the source, which is distributed using the secure overlay. We also show an optimization for this variant, SeGrOM-Hop, which reduces the computation and communication overhead with the help of a per-hop key shared among each head member and their downstream head members in the secure overlay. We continue to use the notations defined in Table 1.

4.4.1. SeGrOM-Group: Using Group Key for Data Encryption and Secure Overlay for Group Key Dissemination

In this protocol, a common group key is maintained among all head members. The group data is encrypted with the group key K_g at the head member of the source, h_s, then disseminated through the multicast tree over the wireless backbone, as seen in Algorithm 2. To avoid the cost of maintaining global membership and changing the group key every time the group changes, we use batching [34], a technique where the source refreshes the group key only periodically instead of refreshing it every time the group membership changes. The advantage of this scheme is its improved performance and simplicity. However, as the key will not be changed immediately when the group changes nodes that leave the group will still be able to decrypt group data until the current key period elapses and a new group key is issued. This results in a partial loss of the forward and backward data secrecy due to the use of periodic group key refreshment.

4.4.2. SeGrOM-Link: Using Per-Packet Keys for Data Encryption and Secure Overlay for Packet Key Dissemination

SeGrOM-Link avoids the partial loss of forward and backward secrecy in SeGrOM-Group. One possible approach is to deliver data directly on the secure group overlay: to forward a data packet, each head member encrypts the data packet with the link key of each of its downstream head members and then forwards the encrypted packets accordingly. However, this approach incurs a large computation and communication overhead, since every data packet needs to be re-encrypted and forwarded by each head member multiple times once for each downstream head member.

To overcome the large overhead, SeGrOM-Link uses per-packet keys to encrypt data. To disseminate a data packet, the head member at the source h_s first selects a random key K_d. It then encrypts the data with K_d and encrypts K_d with the link key of each of its downstream head members. It piggy-backs all the encryptions of K_d to the encrypted data packet, and broadcasts the packet down the multicast tree. When a downstream head member receives the packet, it retrieves the data by first decrypting K_d with its corresponding link key and then using K_d to decrypt the data. To forward the packet downstream, the head member re-encrypts K_d with the link keys of its downstream head members, and replaces the K_d encryptions on the received packet with the new set of encryptions of K_d. Algorithm 3 presents the pseudo-code for SeGrOM-Link.

In this scheme, the encrypted data packet is only broadcast once to all downstream nodes, taking advantage of the wireless broadcast medium. At each head member, only the per-packet keys need to be

Algorithm 3: Global data delivery with SeGrOM-Link.

```
   // Code executed by source head member h_s
   Input: Packet m to be sent from h_s to any h_r
 1 h_s selects packet key K_d;
 2 h_s encrypts m with packet key K_d, result is m_e;
 3 h_s executes forward_data(m_e, K_d)
   // forward_data by head member h_i
   Input: Encrypted data m_e, data key K_d
 4 foreach downstream head member h_j of h_i do
 5 |   h_i encrypts K_d with link key K_ij, result is Ke_j;
 6 |   append Ke_j to m_e
 7 end
 8 deliver the resulting packet to downstream head members.
   // Code executed by h_r when receiving a packet from its upstream head member h_u
   Input: Encrypted data m_e, encrypted data key Ke_r
 9 h_r decrypts Ke_r with link key K_ur, result is K_d;
10 h_r decrypts m_e with packet key K_d, result is m;
11 if (h_r has downstream head member) then
12 |   h_r executes forward_data(m_e, K_d)
13 end
```

re-encrypted for each downstream nodes, since symmetric keys are typically only 128 bits, the computation overhead is also significantly smaller than encrypting data packets directly.

4.4.3. SeGrOM-Hop: Using Per-Packet Key for Data Encryption and Per-Hop Key for Packet Key Dissemination

In SeGrOM-Link, even with the optimization of using per-packet keys, there is still per data packet computation and communication overhead on each head member linear to the number of downstream head members. As data packets are expected to be very frequent, the accumulated computation and communication overhead can be substantial. SeGrOM-Hop optimizes the computation and communication overhead further by having each head member share a *hop key* with all of its downstream head members. Thus, each head member only needs to encrypt K_d with the hop key and deliver the encrypted key once for each data packet, instead of once for each downstream head member. Algorithm 4 presents the pseudo-code for SeGrOM-Hop.

The requirement of forward and backward data secrecy requires the refreshment of the hop key whenever the downstream head member set changes. Since the hop key refreshment involves only adjacent head members, thus incurring only local communication, a straightforward approach, such as encrypting and delivering the new hop key individually for each downstream head member, can be employed. The cost of maintaining a hop key is amortized over all the data packets delivered using that key. Therefore, compared to SeGrOM-Link, SeGrOM-Hop has a lower per data packet overhead.

4.5. Client Member Revocation

Revocation is necessary for many group applications. For example, it is necessary to revoke a member that has been compromised by adversaries. In paid multimedia broadcasting, the content provider needs to revoke membership from customers who default payments. In schemes where the group membership is maintained by one entity (e.g. centralized membership management schemes), members can be easily revoked by the entity that manages the group membership. For example, in the case of single source multicast where the source has the list of the most recent group members, it can revoke the access the data by changing the group key and not delivering the new key to the revoked member. In decentralized schemes, a more general scheme relies on a certificate revocation list (CRL) that includes the name of revoked members. This approach requires the reliable delivery of CRLs to group members, which is costly in a multi-hop wireless

Algorithm 4: Global data delivery with SeGrOM-Hop.

`// Code executed by source head member` h_s
Input: Packet m to be sent from h_s to any h_r
h_s selects packet key K_d;
h_s encrypts m with packet key K_d, result is m_e;
h_s executes forward_data(m_e, K_d)
`// forward_data by head member` h_i
Input: Encrypted data m_e, data key K_d
h_i encrypts K_d with downstream hop key K_{hop}, result is Ke_h ;
h_i sends m_e and Ke_h to downstream head members;
`// Code executed by` h_r `when receiving a packet from its upstream head member` h_u
Input: Encrypted data m_e, encrypted data key Ke_h
h_r decrypts Ke_h with upstream hop key K_{hop}, result is K_d;
h_r decrypts m_e with packet key K_d, result is m;
if *(h_r has downstream head members)* **then**
  h_r executes forward_data(m_e, K_d)
end

environment. Alternatively, the protocol can maintain the node revocation status only at the entity issuing the CRLs (usually a group manager), but then every group join requires a query to the group manager to check the revocation status of the joining member. As group joins are expected to be frequent, this approach can incur a significant delay and overhead in a multi-hop wireless environment.

We propose a more efficient revocation scheme, SeGrOM-Revoke, which combines the benefits of both approaches: It eliminates the need of reliable broadcast of CRLs to all group members and also requires only localized traffic for checking revocation status. We assume that most member clients move around a region that can be covered by a small set of access routers, which are referred to as the client's *home routers*. This assumption is valid for most application scenarios, such as real-time conferencing, multimedia broadcasting, and multi-player gaming, where most active group members stay in some local region. SeGrOM-Revoke exploits such locality of client movements in WMNs to support more efficient member revocations. The main idea is to maintain the revocation status of a client at the members associated with the client's home routers. Thus, checking the revocation status of a member requires only querying a member associated with a local home router of the member, while revoking a member requires only delivering the revocation notice to members associated with the home routers of the revoked member.

Scheme Details. Prior to joining the group, a client first selects a set of routers that cover its movement area, which can be discovered with scoped local flooding, as its home routers. Recall that the group manager is the central entity responsible for authorizing group members, issuing member certificates, and revoking group members (Section 3). When requesting a member certificate, the client presents its selected home router set to the group manager, who then includes them in the member certificate.

When the group manager decides to revoke a member certificate, it sends a signed revocation notice to the head member of each home router of the revoked client, which then disseminates it to other members associated with the same router. Hence, all the members on the home routers of a member client maintain the revocation status for the client.

When a client joins a group, the upstream head member needs to check whether the new member has a valid member certificate that has not been revoked. To do so, it first verifies the presented group member certificate. Upon verification, it contacts a head member of one of the home routers listed in the member certificate to verify the revocation status of the client. Since it is expected that a member client joins the group via one of its home routers or some router close to its home routers, the revocation verification process incurs only local traffic.

A caveat in the join process is that since only clients that are currently in the group are trusted, the upstream head member also needs to verify that the responding party is a current group member. For proof of the current membership, we present a challenge-response scheme that relies upon the single secret shared

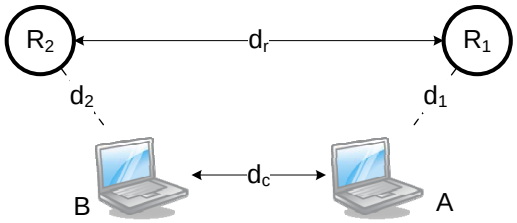


Figure 3: The newly joined member client (A), its closest member client (B), and their associated access routers (R_1 and R_2). The symbols (d_r, d_c, d_1, d_2) denote the distance between the respective entities.

among all group members – the data itself. The challenging member sends a window of sequence numbers for recent packets to the target node, which responds with a signed hash of one of the packets. Since only current group members have access to current group data, the correct hash value proves the current membership of the node. Allowing the target node to select one from a window of sequence numbers addresses the lossy environment of wireless networks where the target node may have lost some of the recent packets.

In the case that no member clients exist on the home routers of the joining client, the group manager is contacted for revocation status, which involves global communication. However, as shown in the experiments (Section 6.3), such cases are infrequent in most situations. Performance can be further optimized for roaming clients that move far away from their home region for an extended period by issuing them new member certificates with updated home router sets.

5. Performance Analysis

In this section we compare the join and leave bandwidth cost and latency of SeGrOM protocols with centralized schemes, where the source node is contacted for every join and leave. Since the communication among backbone routers is expected to be a bottleneck in most applications and the local communication between clients and their access router are common in both approaches, we focus the analysis on the cost of the communication among wireless routers. We discuss only member joins as member leaves are analogous.

We assume a random geometric graph model for the analysis, namely, both wireless routers and member clients are uniformly randomly distributed in a two-dimensional unit square. Denote the number of routers as n and the number of member clients as m. The radio transmission range of the routers is such that the routers form a connected graph with average degree $O(\log n)$[1]. Each client has at least one router in its range and is associated with the router closest to it.

Since both bandwidth cost and latency are directly proportional to the communication path length, in the following we first derive the expected communication path length in SeGrOM and the centralized approach, respectively. We then determine the ratio of bandwidth and latency savings using the ratio of the communication path length of the two approaches.

5.1. Communication Path Length for SeGrOM Join

In SeGrOM, if a new client joins the group with a router that has existing member clients, the join is handled by the local head member and no communication among backbone routers is required. Thus, we only consider the event that the new client joins with a router with no existing members. Let p be the probability of such event, since each member client has an equal probability of associating with any of the routers, we have

$$p = (1 - \frac{1}{n})^m.$$

[1]In random geometric graph, the average degree of $O(\log n)$ is sufficient for connectivity while maintaining reasonable density [35].

Let d_c be the random variable for the distance between the new client and the closest member client, d_1 and d_2 be the distances between these two members and their access routers, and d_r be the distance between the two routers, as shown in Fig. 3. We then have

$$d_r \leq d_c + d_1 + d_2 \tag{1}$$

Lemma 1. *Uniformly randomly place a point A and n other points in a unit square, let D be the minimum distance between A to one of the n points, then*

$$E[D] \leq 2n\pi \int_0^\infty x^2 e^{-n\pi x^2} dx.$$

Proof. See appendix. □

Therefore, by Lemma 1, we have

$$E[d_c] \leq 2m\pi \int_0^\infty x^2 e^{-m\pi x^2} dx,$$
$$E[d_1] = E[d_2] \leq 2n\pi \int_0^\infty x^2 e^{-n\pi x^2} dx.$$

In SeGrOM, the router R associated with the new member client joins the multicast tree by contacting the closest router R' with existing member clients. Let D_R be the distance between router R and router R', then

$$D_R \leq d_r \leq d_c + d_1 + d_2.$$

Hence by the linearity of expectation, we have

$$E[D_R] \leq E[d_c] + 2E[d_1]. \tag{2}$$

Let H_R be the length of the shortest path between R and R'. Given a distance D_R, since the routers are uniformly distributed, we have $E[H_R|D_R]$ being proportional to D_R, that is $E[H_R|D_R] = D_R g(n)$, where $g(n)$ is some function of n that reflects the density of the network. Therefore,

$$E[H_R] = E[E[H_R|D_R]] = E[D_R]g(n). \tag{3}$$

Therefore, let H be the communication path length for joining the group in SeGrOM, combining Equation 2 and 3, we have

$$\begin{aligned} E[H] &= pE[H_R] \\ &= pE[D_R]g(n) \\ &\leq p(E[d_c] + 2E[d_1])g(n) \end{aligned} \tag{4}$$

5.2. Communication Path Length for Centralized Join

Let D'_R be the distance between the router associated with the joining client and the router associated with the source client. Since both the routers and clients are uniformly randomly distributed, the routers associated with the source client and the new client are uniformly distributed in the unit square.

Lemma 2. *The expected distance between two random points in a unit square is $\frac{1}{15}(2 + \sqrt{2} + 5\ln(1 + \sqrt{2}))$ (as shown in [36]).*

Thus by Lemma 2, we have

$$E[D'_R] = \frac{1}{15}(2 + \sqrt{2} + 5\ln(1 + \sqrt{2})).$$

Let H'_R be the path length between the two routers. Similar to the argument in the SeGrOM case, we have

$$E[H'_R] = E[D'_R]g(n). \tag{5}$$

5.3. Bandwidth Cost and Latency Ratio for Join Between Centralized Schemes and SeGrOM

Combining Equation 4 and 5, the ratio of the expected path length R_{pl} for join between centralized approach and SeGrOM is

$$\begin{aligned} R_{pl} &= \frac{E[H'_R]}{E[H]} \\ &= \frac{E[D'_R]g(n)}{pE[D_R]g(n)} \\ &\geq \frac{E[D'_R]}{p(E[d_c]+2E[d_1])} \\ &= \frac{\frac{1}{15}(2+\sqrt{2}+5\ln(1+\sqrt{2}))}{2p\pi(m\int_0^\infty x^2e^{-m\pi x^2}dx + 2n\int_0^\infty x^2e^{-n\pi x^2}dx)} \end{aligned}$$

Now we show the following theorem.

Theorem 1. *Let R_l and R_b be the ratio of expected latency and the ratio of expected bandwidth cost, respectively, for join between the centralized approach and SeGrOM, then*

$$\begin{aligned} R_l &= R_{pl} \\ R_b &\geq R_{pl}/D, \end{aligned}$$

where D is the average degree of the backbone network.

Proof. Since join latency is directly proportional to the communication path, we have $R_l = R_{pl}$.

In SeGrOM a group join to a router empty of members also involves communication with all the downstream head members to maintain the group overlay. Let d be the number of downstream head members for a group join, we have $E(d) \leq D$. Therefore, the expected ratio of the join bandwidth cost $R_b = R_{pl}/E(d) \geq R_{pl}/D$. □

Figure 4(a) and 4(b) plot the latency ratio and the lower bound for the bandwidth cost ratio with respect to the number of member clients when the number of routers $n = 100$ and $n = 200$ and the average degree is $\log n$. From the figures, we can see that both ratios increase when the density of member clients gets higher, which indicates that the improvement of SeGrOM over centralized schemes for joins and leaves becomes more significant for groups with higher client density. We also see that increasing n from 100 to 200 decreases both ratios. This is because as n increases, there is a smaller chance of handling join/leave by local head members. In addition, the number of downstream head members also increases, resulting in a higher bandwidth cost for join/leave in SeGrOM.

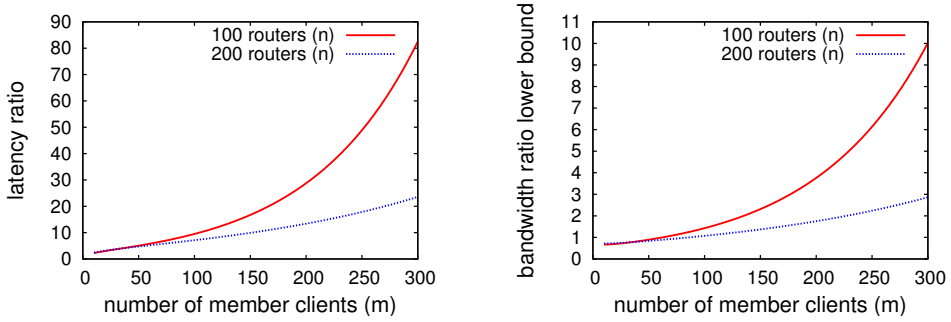
6. Experimental Evaluation

In this section, we present an evaluation of the proposed protocols. We first describe our experimental methodology, including a baseline protocol, referred to as W-LKH. We then compare the performance and overhead of our protocols against the baseline protocol. Finally, we evaluate the overhead of the SeGrOM-Revoke revocation protocol.

6.1. Experimental Methodology

We implemented our protocols using the *ns2* network simulator [13] (version 2.26) with CMU Monarch extensions. The MAODV implementation is provided by Zhu et al [37].

Wireless routers are simulated with nodes equipped with IEEE 802.11 radio, 2Mbps physical bandwidth and 250-meter nominal range. 100 routers are randomly placed in a $1500m \times 1500m$ area. The mobile clients are also randomly placed in the area and are associated with the nearest router. We assume the local communication between mobile clients and their access router is on a different channel than the channel



(a) Latency ratio (b) Bandwidth cost ratio lower bound

Figure 4: The latency and bandwidth cost ratio in a join operation between a centralized scheme and SeGrOM

used on the backbone network, thus it does not interfere with the backbone communication. We assume the communication between the mobile clients and their access routers is reliable with a fixed latency, set empirically at 4ms.

In the beginning of a simulation, the source client and 100 member clients are placed at random positions and join the group sequentially at the rate of one join per two seconds. For experiments considering group dynamics we use Poisson process to model the member join and leave events, based on previous studies [32, 38, 39]. We set the join and leave rates to be equal so that the group size remains stable. For each join event, the new client joins from a random position; for each leave event, a random member node is selected to leave the group. The duration of each simulation is 1000 seconds. The source client starts sending data after the initial member joins are completed. The packet size is 256 bytes, and the packet rate is varied. For experiments that examine the effect of group dynamics, the data rate is fixed at 5 packets/second, to optimize the performance of MAODV.

We compare our protocols with a centralized protocol adapted to cope with the high loss ratio and latency existent in multi-hop wireless networks. The protocol is based on the well-known LKH [34] protocol and is referred as W-LKH. W-LKH uses logical key graphs to minimize the number of encryptions performed by the source. It also incorporates batching [34] to minimize the communication cost, and reliable hop-by-hop key delivery to cope with lossy links.

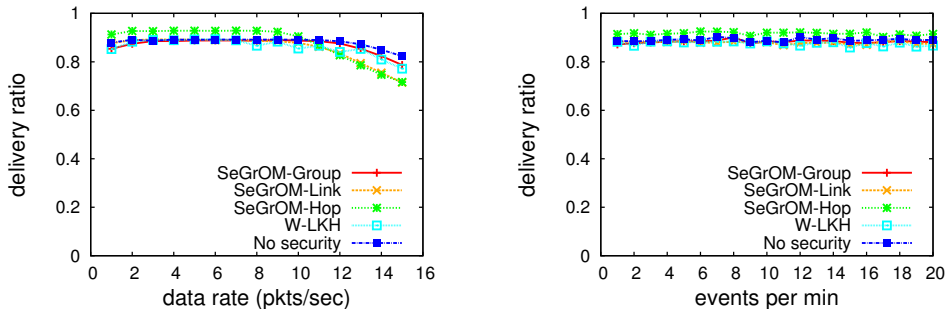
For protocols that use batching (W-LKH and SeGrOM-Group), a balanced key refreshment period of 30 seconds was chosen based on previous studies [6]. We also assume in all the protocols the size of symmetric keys is 128 bits, the size of public/private keys is 1024 bits, and the computation delay for PKI signatures is 4ms.[2] All data points plotted are the average of 10 runs with different random router and client topologies and group join and leave events.

We compare the protocols using the following metrics:

- *Delivery ratio:* The delivery ratio is defined as the fraction of data packets that are received and decrypted by a group member node out of all the data packets that are broadcast by the source during the time when the node is a group member. The delivery ratio measures the data goodput received by the upper layer application.

- *Computation, bandwidth and latency overhead of join and leave events, and the overall bandwidth overhead:* Since mobile clients and wireless routers are expected to be limited in computation power, we evaluate the computation cost of different protocols. To see how our protocols cope with the limited bandwidth in WMNs, we evaluate their bandwidth overhead. Finally, to see how responsive our protocols are to upper layer applications, we evaluate the latency of join and leave events.

[2]This value is based on running the 1024-bit RSA implementation of `openssl` on a 3GHz Intel Pentium IV computer.



(a) Delivery ratio *vs.* data rate

(b) Delivery ratio *vs.* group dynamics

Figure 5: Delivery ratio of SeGrOM protocols

6.2. Protocol Performance and Robustness

Figure 5(a) and 5(b) show the delivery ratio for different protocols for different data rates and group dynamics. We observe that for all data rates and group dynamics examined, all proposed secure multicast protocols maintain a high delivery ratio similar to the case with no security mechanisms. Surprisingly, we observe that SeGrOM-Hop even has a slightly higher delivery ratio than the no security case for lower data rates. A more in-depth analysis reveals that the local hop key maintenance in SeGrOM-Hop tends to eliminate weak links in the multicast tree that persist in the bare MAODV case, having the unexpected benefit of optimizing the multicast tree and resulting in a better delivery ratio.

We also experimented with random node and link failures to examine the robustness of the protocols. The resulting performance is similar to the results shown for the case with no artificial failures. We omit these graphs due to the limited space.

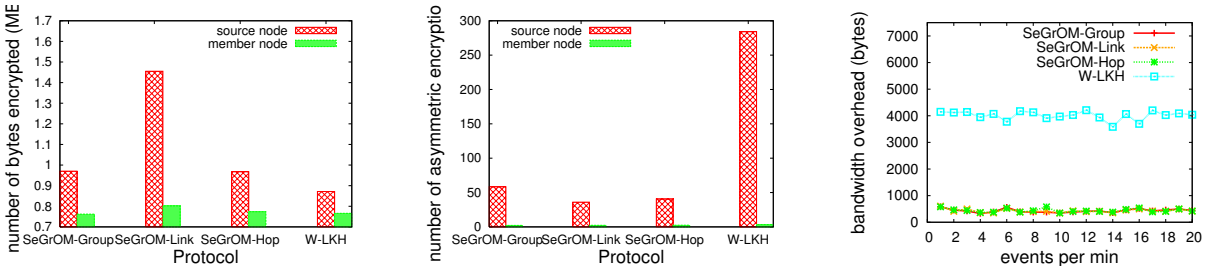
6.3. Protocol Overhead

Computation overhead. Figures 6(a) and 6(b) show the computation overhead due to cryptographic operations at the source node and a randomly selected member node for our protocols and W-LKH. The source sends at a data rate of 5 packets/second (10kbps) to optimize MAODV performance. The group dynamics used were 5 joins and 5 leaves per minute.

For symmetric encryption overhead, we observe that SeGrOM-Link has much higher overhead than the other protocols, especially at the source node. This is because SeGrOM-Link requires per data packet computation overhead linear to the number of children of the node. The optimizations in SeGrOM-Hop successfully reduce the overhead making it comparable to other protocols.

For asymmetric encryption overhead, we observe that W-LKH has a significantly higher number of encryptions performed by the source node than the other protocols, due to the centralized handling of joins and leaves, each of which requires asymmetric encryptions. Since asymmetric encryptions are computation intensive operations, the centralization of such encryptions in W-LKH introduces a potential performance bottleneck at the source, especially at high group dynamics. It also allows for potential DoS attacks that aim at exhausting the computation resource of source nodes.

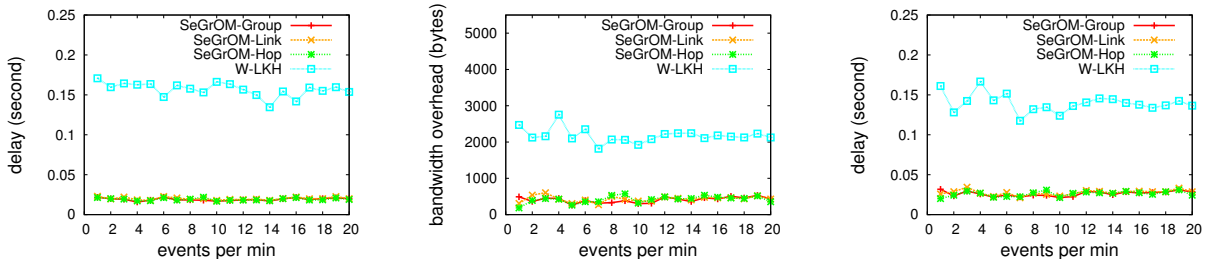
Bandwidth overhead and latency. Figures 6(c), 6(d) and Figures 6(e), 6(f) show the bandwidth overhead and latency for the join and leave events, respectively, for different levels of group dynamics. To decouple the cost of a join event from the revocation status verification, we assume most nodes join the network from their home routers. From these graphs, we first observe that all proposed protocols maintain similar bandwidth overhead and latency for different levels of group dynamics. We also observe that W-LKH has much higher bandwidth overhead and latency for join and leave than SeGrOM-based protocols (e.g. about 8 times more bandwidth overhead for a join event), demonstrating the benefits of decentralized membership management in SeGrOM.



(a) The symmetric encryption overhead

(b) The asymmetric encryption overhead

(c) Join bandwidth overhead



(d) Join latency

(e) Leave bandwidth overhead

(f) Leave latency

Figure 6: Computation overhead and join/leave overhead of SeGrOM protocols

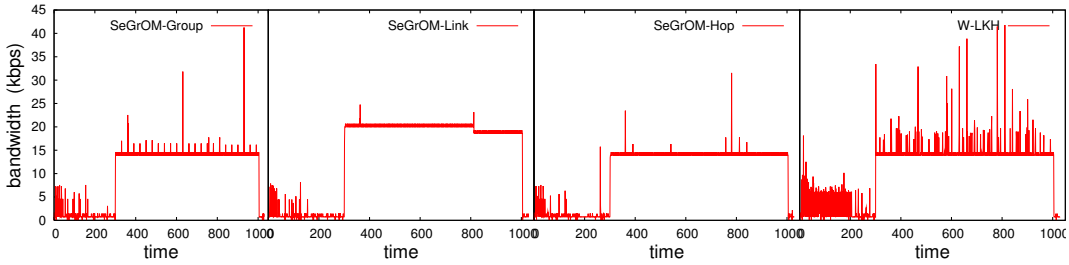


Figure 7: Peak bandwidth of SeGrOM protocols

Compared to the theoretical analysis results in Section 5, we observe that the experimental latency ratio (around 8–9) is similar to the result derived from the analysis (around 10, see Fig. 4(a) for the case $n = 100, m = 100$)[3]. We also observe that the experimental bandwidth cost ratio of W-LKH over SeGrOM is much higher than the theoretical analysis result (see Fig. 4(b) for the case $n = 100, m = 100$). This is due to the overestimation of the number of downstream head members in the analysis, which causes the underestimation of the bandwidth cost ratio.

Peak bandwidth. Figure 7 shows the bandwidth consumed at the source node over time for different protocols for a simulation run with a data rate of 5 packets/second and group dynamics of 5 joins and 5 leaves per minute. From these graphs, we can see that SeGrOM-based protocols consume a relatively stable bandwidth at the source over time, while W-LKH exhibits high variability of bandwidth consumption. The reason for the high peak bandwidth requirement of W-LKH is two-fold. First, the size of the rekey packets in W-LKH is relatively large, since potentially many keys targeted for different members needs to be included. Second, all join and leave requests require communication with the source. Since high bandwidth peaks can

[3]The slightly lower ratio for the experimental results is because the theoretical analysis ignores the computation and local communication latency from routers to head members, which is slightly higher in SeGrOM.

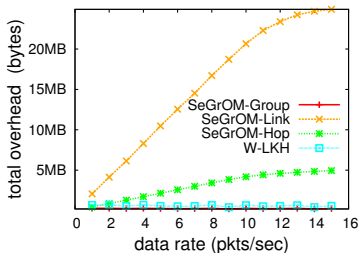


Figure 8: Total bandwidth overhead *vs.* data rates

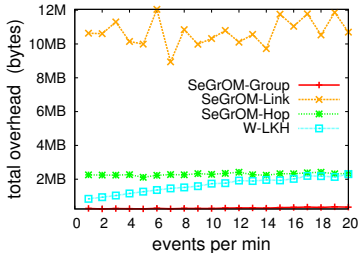


Figure 9: Total bandwidth overhead *vs.* group dynamics

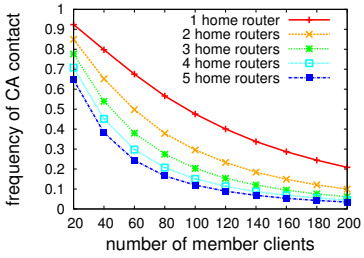


Figure 10: The frequency of CA contact required for a join in a network with 100 routers.

cause packet loss and network congestion, W-LKH is less favorable than the SeGrOM-based protocols in this respect.

Total bandwidth overhead. For an overview of all bandwidth overhead introduced by the secure multicast protocols, Figures 8 and 9 show the average total bandwidth overhead due to the protocols for an entire simulation session for different data rates and group dynamics, respectively.

We first observe that the bandwidth overhead for both SeGrOM-Link and SeGrOM-Hop increases linearly with the data rate. However, the rate of increase for SeGrOM-Hop is significantly smaller than SeGrOM-Link, allowing its bandwidth overhead to remain comparable to other protocols while that of SeGrOM-Link is much higher. This difference shows the effectiveness of the hop key in SeGrOM-Hop for reducing bandwidth overhead. From Figure 9, we can also observe that for SeGrOM protocols, the total bandwidth overhead remains quite stable for different levels of group dynamics, while for W-LKH the overhead increases linearly with group dynamics, again due to the global messages required for handling membership changes.

Overhead of SeGrOM-Revoke. In SeGrOM-Revoke, the main bandwidth and latency cost occurs when the CA must be contacted for revocation status verification due to the absence of member clients on the home routers of the joining client, or the absence of CRL in those member clients. Fig 10 shows the frequency of CA contact occurrence in a network with 100 routers for stabilized networks of different group sizes and different home router set sizes. As can be seen from the figure, the frequency is quite low when the number of clients is reasonably large.

7. Conclusion

In this paper, we explored different design choices for solving the problem of secure multicast service for WMNs. We proposed several secure group multicast protocols that employ decentralized group membership, promote localized communication, and exploit the wireless broadcast nature, to efficiently accommodate dynamic group changes and reduce communication overhead. We compare our protocols with a baseline centralized protocol and discuss the trade-offs among different design choices. Our results indicate that:

- Adding application-level data confidentiality to group communication in WMNs does not affect the performance of the system. The bottleneck of achievable data rate is not the data confidentiality mechanism but the underlying network bandwidth.
- Our decentralized protocols show smaller computation and bandwidth overhead and latency in dynamic groups where the set of receivers changes frequently. In addition, our protocols show a smaller peak overhead than the centralized baseline protocol for dynamic groups.
- Using a different encryption key per packet and hop key for delivering the data encryption key exhibits the best balance between security and overhead.

References

[1] I. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Computer Networks Journal*, March 2005.

[2] C. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," *Trans. Netw.*, vol. 8, no. 1, 2000.

[3] A. Perrig, D. Song, and J. D. Tygar, "ELK, a new protocol for efficient large-group key distribution," in *S&P*, 2001.

[4] X. Zhang, S. Lam, and H. Liu, "Efficient group rekeying using application layer multicast," in *ICDCS '05*.

[5] C. Abad and I. Gupta, ""Adding confidentiality to application-level multicast by leveraging the multicast overlay"," in *Proc. of ADSN '05*, 2005.

[6] R. Torres, X. Sun, A. Walters, C. Nita-Rotaru, and S. Rao, "Enabling confidentiality of data delivery in an overlay broadcasting system," in *INFOCOM 2007*, 2007.

[7] W. Du, J. Deng, Y. Han, and P. Varshney, "A key predistribution scheme for sensor networks using deployment knowledge," *IEEE TDSC*, vol. 3, no. 1, 2006.

[8] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. of S&P*, 2003.

[9] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. of CCS '02*, 2002.

[10] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN: An efficient group rekeying scheme for secure multicast in ad-hoc networks," *Mobiquitous*, vol. 00, 2004.

[11] R. Balachandran, B. Ramamurthy, X. Zou, and N. Vinodchandran, "CRTDH: an efficient key agreement scheme for secure group communications in wireless ad hoc networks," in *Proc. of IEEE ICC '05*.

[12] T. Kaya, G. Lin, G. Noubir, and A. Yilmaz, "Secure multicast groups on ad hoc networks," in *Proc. of SASN '03*, 2003.

[13] "The network simulator - ns2." http://www.isi.edu/nsnam/ns/.

[14] X. Li, Y. Yang, M. Gouda, and S. Lam, "Batch rekeying for secure group communications," in *Proc. of WWW '01*, 2001.

[15] C. Wong and S. Lam, "Keystone: A group key management service," in *Proc. of ICT '00*, 2000.

[16] X. Zhang, S. Lam, D.-Y. Lee, and Y. Yang, "Protocol design for scalable and reliable group rekeying," *ToN*, vol. 11, no. 6, 2003.

[17] X. Zhang, S. Lam, and D.-Y. Lee, "Group rekeying with limited unicast recovery," *Comput. Networks*, vol. 44, no. 6, 2004.

[18] Y. Yang, X. Li, X. Zhang, and S. Lam, "Reliable group rekeying: a performance analysis," in *SIGCOMM '01*.

[19] S. Mittra, "Iolus: a framework for scalable secure multicasting," in *Proc. of ACM SIGCOMM '97*, 1997.

[20] Y. Kim, A. Perrig, and G. Tsudik, "Simple and fault-tolerant key agreement for dynamic collaborative groups," in *CCS '00*, (New York, NY, USA), pp. 235–244, ACM, 2000.

[21] Y. Kim, A. Perrig, and G. Tsudik, "Communication-efficient group key agreement," in *IFIP/Sec '01: Proceedings of the IFIP TC11 Sixteenth Annual Working Conference on Information Security*, (Deventer, The Netherlands, The Netherlands), pp. 229–244, Kluwer, B.V., 2001.

[22] M. Steiner, G. Tsudik, and M. Waidner, "Cliques: A new approach to group key agreement," in *in IEEE International Conference on Distributed Computing Systems*, pp. 380–387, IEEE Computer Society Press, 1998.

[23] W.-P. Yiu and S.-H. Chan, "SOT: secure overlay tree for application layer multicast," in *ICC '04*.

[24] C. Abad, I. Gupta, and W. Yurcik, "Adding confidentiality to application-level multicast by leveraging the multicast overlay," in *Proc. of ADSN in ICDCSW '05*, 2005.

[25] S. Zhu, C. Yao, D. Liu, S. Setia, and S. Jajodia, "Efficient security mechanisms for overlay multicast-based content distribution.," in *ACNS*, 2005.

[26] Y. Sun, W. Trappe, and K. J. R. Liu, "A scalable multicast key management scheme for heterogeneous wireless networks," *IEEE/ACM Trans. Netw.*, vol. 12, no. 4, pp. 653–666, 2004.

[27] S. Roy, V. Addada, S. Setia, and S. Jajodia, "Securing MAODV: Attacks and countermeasures," in *Proc. of SECON '05*, 2005.

[28] R. Curtmola and C. Nita-Rotaru, "BSMR: Byzantine-resilient secure multicast routing in multi-hop wireless networks," in *In IEEE SECON 2007*.

[29] Y. Zhang and Y. Fang, "A secure authentication and billing architecture for wireless mesh networks," *Wirel. Netw.*, vol. 13, no. 5, pp. 663–678, 2007.

[30] Y. Zhang and Y. Fang, "ARSA: An attack-resilient security architecture for multihop wireless mesh networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, pp. 1916–1928, Oct. 2006.

[31] E. Royer and C. Perkins, "Multicast operation of the ad-hoc on-demand distance vector routing protocol," in *MobiCom '99*.

[32] K. Srip., A. Ganjam, B. Maggs, and H. Zhang, "The feasibility of supporting large-scale live streaming applications with dynamic application end-points," in *SIGCOMM*, 2004.

[33] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, 1976.

[34] X. S. Li, Y. R. Yang, M. G. Gouda, and S. S. Lam, "Batch rekeying for secure group communications," in *WWW '01*.

[35] S. Muthukrishnan and G. Pandurangan, "The bin-covering technique for thresholding random geometric graph properties," in *SODA '05*, 2005.

[36] B. Gaboune, G. Laporte, and F. Soumis, "Expected distances between two uniformly distributed random points in rectangles and rectangular parallelpipeds," *The Journal of the Operational Research Society*, vol. 44, no. 5, 1993.

[37] Y. Zhu and T. Kunz, "MAODV implementation for NS-2.26," Technical Report SCE-04-01, Carleton University.

[38] Y.-H. Chu, A. Ganjam, E. Ng, S. Rao, K. Srip., J. Zhan, and H. Zhang, "Early experience with an internet broadcast system based on overlay multicast," in *USENIX 04*.

[39] K. Almeroth and M. Ammar, "Collecting and modeling the join/leave behavior of multicast group members in the mbone," in *Proc. of (HPDC) '96*, 1996.

Proof of Lemma 1

Proof. Ignoring boundary effect, the number of points that fall into a circle of radius x with center at A can be approximated with Poisson distribution with $\lambda = n\pi x^2$. Thus we obtain the CDF of D,

$$\begin{aligned} F_D(x) &= Pr(D \leq x) \\ &= 1 - Pr(D > x) \\ &= 1 - Pr(\text{no client in the circle of radius } x) \\ &= 1 - e^{-n\pi x^2} \end{aligned}$$

Thus, the probability density function of D is

$$f_D(x) = \frac{dF_D(x)}{dx} = 2n\pi x e^{-n\pi x^2},$$

hence

$$E[D] \leq \int_0^\infty x f_D(x) dx = 2n\pi \int_0^\infty x^2 e^{-n\pi x^2} dx.$$

Note that ignoring boundary effect results in a lower bound on the density of the points, thus the expected minimum distance computed is an upper bound on the actual density. □