Performance Characteristics of Region-Based Group Key Management in Mobile Ad Hoc Networks

Ing-Ray Chen[†] Jin-Hee Cho[†] Ding-Chau Wang[*]

[†] Virginia Tech
Department of Computer Science
{irchen, jicho}@vt.edu

[*] Southern Taiwan University of Technology
Department of Information Management
zh9@mail.stut.edu.tw

Abstract

We propose and analyze a scalable and efficient region-based group key management protocol for secure group communications in mobile ad hoc networks. For scalability and dynamic reconfigurability, we take a region-based approach by which group members are broken into region-based subgroups and leaders in subgroups securely communicate with each other to agree on a group key in response to membership change and member mobility events. We show that the secrecy requirement for group communication is satisfied. Further, there exists an optimal regional size that minimizes the total network communication cost as a result of efficiently trading inter-regional vs. intra-regional group key management overheads. We give an analytical expression of the cost involved which allows the optimal regional size to be identified, when given a set of parameter values characterizing a group communicating system in mobile ad hoc networks.

1 Introduction

Many mobile wireless applications nowadays are based on secure group communication [1, 6] by which data is encrypted using an encryption key (called a *group key* hereafter). When a member joins a group, the group key is rekeyed to ensure that the new member cannot decrypt previous messages. This is a requirement known as *backward secrecy* [4]. When a member leaves the group, the group key is rekeyed to ensure that future communications cannot be decrypted by the leaving member, a requirement known as *forward secrecy*. The algorithms that deal with the distribution, updating, and revocation of the group key are popularly known as *group key-management protocols*.Conceivably, as the number of group members becomes large, group key management can incur significant overheads and cause a potential system performance bottleneck. In this paper, we propose a reliable and secure region-based group key management protocol for secure group communication in mobile ad hoc networks (MANET). For scalability and dynamic management, we propose a two-level hierarchical key management architecture adopted from the IETF Group Key Management Architecture [10] to efficiently and securely distribute keys and the Contributory Key Agreement (CKA) protocol [1,2,3,4] for key generation without using a centralized key server. We break a group into region-based subgroups with leaders in subgroups communicating with each other to agree on a group key in response to membership change and member mobility events. In addition to showing that the forward and backward secrecy requirements of secure group communication are satisfied, we identify optimal settings of our protocol to minimize the overall communication cost due to group key management, when given a set of parameter values characterizing the operational and environmental conditions of a group communicating system in MANET.

The rest of this paper is structured as follows. Section 2 surveys related work. Section 3 gives the system model and describes the proposed region-based group key management protocol. Section 4 develops a performance model to evaluate performance characteristics of region-based group key management protocols compared with non-regional counterparts. Section 5 analyzes costs involved in group key management and identifies optimal regional sizes under which the overall communication cost for group key management is minimized while still satisfying secrecy requirements, with physical interpretations given. Finally Section 6 concludes the paper and outlines the future work.

2 Related Work

Zhang et al. [10] examined the effect of mobility on secure rekeying of group communication by using a hierarchical key-distribution framework. They proposed several rekeying algorithms that preserve secrecy properties as members move within the hierarchy. However, they assumed regions in a group that there exists a key server for rekeying operations, which is not suitable for mobile ad hoc networks. Our approach does not use a key server and we identify optimal regional sizes to minimize the group key management cost.

Amir et al. [3] presented a robust contributory key agreement (CKA) protocol resilient to group membership changes. Their protocol is based on group Diffie-Hellman contributory key agreement to extend the services of a group communication system to provide virtual

synchrony semantics. Amir et al. [1] showed group communication systems can be enhanced with security services without sacrificing robustness and performance. These works are not based on hierarchical group key management. In our paper, we apply CKA in two levels, with one at the inter-regional level and one at the intra-regional level. Their algorithm can be considered as an extreme case in which there is only one region that connects all group members, which we use as the baseline case for performance comparison. Amir et al. [2] presented a performance evaluation of distributed key management techniques (for collaborative peer groups) integrated with a reliable group communication system. The work, however, is mainly targeted for wired networks. Kim et al. [5] proposed a new group key agreement protocol for secure group communications to tradeoff computation for communication efficiency. Their work extends a CKA protocol [8] to handle dynamic groups and network failures. Again such a CKA protocol developed can be considered as a special case in which there is only a single region in the group.

Rodeh et al. [7] described an efficient algorithm for the management of group keys for group communication systems. Their algorithm is based on the use of a key graph maintained in a distributed and collaborative manner by group members. Their work does not consider the use of a hierarchical group key management structure for scalability of key management, nor does it consider mobility-induced key management issues in mobile ad hoc networks.

3 System Model

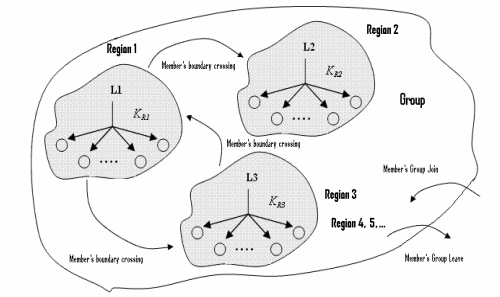

Figure 1: Region-Based Group Key Management.

Figure 1 demonstrates conceptually how a group may span several geographical regions and how members located in separate regions would behave. A region can be of any size and members can move across regions at will. The regional size is an important parameter that will determine the key management cost and we aim to determine the optional regional size. In our protocol, a leader communicates with the members in the same region using a *regional key*, K_R. All leaders in the group use a *leader key*, K_{LR}, for communications among leaders. A *group key*, K_G, is derived from the leader key K_G = MAC (K_{LR}, c), where K_{LR} is a leader key and c is a counter to be incremented whenever a group membership change event occurs. The *group key* (K_G) is used for secure data communications among group members.

These three keys are rekeyed for secure group communications depending on events that occur in the system. The *leader key* (K_{LR}) is rekeyed whenever there is a leader change, including a leader crossing a regional boundary or leaving the group, and a leader failure. A *regional key* (K_R) is used for communications between a leader and the members in the same region and is used by a regional leader to distribute K_G to its members. The *regional key* (K_R) is rekeyed whenever there is a regional membership change event including local member group join/leave, node failure, and local regional boundary crossing event, to preserve secrecy. Table 1 below summarizes the notation used.

Symbol	Meaning
K_G	Group key.
K_{RL}	Leader key.
K_{Ri}	Regional key in region *i*.
RV	Regional view.
LV	Leader view.
GV	Group view.
L_i	A leader in region *i*.

Table 1: Notation.

In addition to maintaining secrecy properties, we also maintain membership consistency [9] through *membership views*. Three membership views are introduced: (a) *Regional View (RV)* contains regional membership information including regional members' ids and regional members' location information, (b) *Leader View (LV)* contains leaders' ids and location information, and (c) *Group View (GV)* contains group membership information that includes members' ids and location information. Figure 2 illustrates the views kept by a leader vs. those by a member.

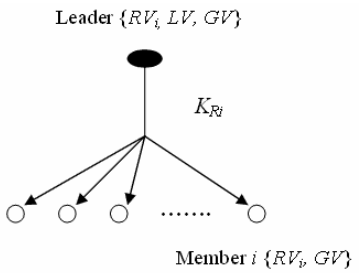

Figure 2: Views for Leaders and Members.

Our proposed protocol preserves the all secrecy properties [4]. *Group Key Secrecy*, that is, it is computationally infeasible for a passive adversary to discover any group key, is guaranteed since we generate a group key using secure MAC. *Forward Secrecy*, i.e., a passive adversary who knows a contiguous subset of old group keys cannot discover any subsequent group key, and *Backward Secrecy*, i.e., a passive adversary who knows a contiguous subset of group keys cannot discover previous group key, are guaranteed because a group key is changed upon a group join or leave event. Finally, *Key*

Independence, that is, a passive adversary who knows a proper subset of group keys cannot discover any other group key, is guaranteed since our group key is generated using MAC with two different inputs, a leader key and a fresh counter, which guarantee key independence. Below we describe our region-based key management protocol for MANET in response to events that may occur in the system.

Group join: When a new member, say *A*, joins the group, *A* periodically beacons a "hello" message including its id and location information to inform its intention to join the group. Some neighboring nodes receiving the beacon forward the "hello" message to their regional leader or a regional leader may receive it directly from *A*. The regional leader receives the join message and updates its regional membership list. Then, the leader broadcasts a new join member's id and location information to its members so that its members are able to update their regional views. Also, the regional leader informs a new join member's information to all other leaders so other leaders are able to disseminate the membership change to all their corresponding members. Then, a new regional key is generated and distributed by a CKA protocol among the regional members. Since a join event incurs a group membership change, all leaders will generate a new group key, with each leader distributing the new group key to the members in its region. In summary, when a new member joins the group, a regional key and a group key are rekeyed and the corresponding regional view and group view are updated to maintain consistent views.

Group leave: When a current non-leader member, say, *B*, leaves the group, *B* notifies its leaving intention to its regional leader. When the leader receives the leaving intention message from *B*, it updates its regional view and disseminates the updated regional view to its members. Since a group leave event instigates regional membership change, a new regional key is generated by executing a CKA protocol and distributed to the regional members. Next, the leader informs the change membership information to all other leaders. After all leaders receive the information on the current leave event, they also broadcast the changed group view to all their members. Finally, all leaders autonomously regenerate a group key and distribute it to their corresponding members.

Group leave by a leader member: When a leader (who is a member) leaves the group, a leader key also should be changed. Thus, in addition to all operations required in the above case for the non-leader member leave, a new leader is elected to replace the leaving leader. Since this involves a leader membership change, all leaders including the new leader elected will execute a CKA protocol to generate a new leader key. Then each leader autonomously generates a new group key and distributes the new group key to members using the regional key.

Boundary crossing by a non-leader member: If a non-leader member crosses a regional boundary, for example, from region *i* to region *j*, a regional membership change occurs in both regions *i* and *j*. Thus, the regional keys in the two involved regions are respectively rekeyed based on CKA and the members' views in these two regions are updated. Since the mobility event changes neither the leader view nor the group view, no leader or group view updates are necessary.

Boundary crossing by a leader member: If a leader member crosses a regional boundary from *i* to *j*, there is a leadership change in addition to all operations considered in the event of boundary crossing by a non-leader member. Thus, as in the group leave by a leader member event, a new leader in the departing region is elected, the leader key is rekeyed among all leaders, and the leader view is updated among all leaders.

Group member disconnection and reconnection: Members may disconnect voluntarily (i.e. turn power off for energy saving) or involuntarily (i.e. obstructions or jamming, etc.). To detect a member failure in the group, each mobile host periodically sends an "I-am-alive" beacon message to its leader so that the leader is aware of which members are in its region. If a leader does not hear the beacon for a certain time period (Threshold-T) from a member, it considers the member as disconnected and a group leave event is instigated. If the member being disconnected is a leader, a new leader is elected by following a new leader election protocol. Temporarily disconnected member nodes can later reconnect and rejoin the group. Our protocol treats reconnections as group join events.

Leader election: A group leave, a boundary crossing or a disconnection by a leader member triggers a new leader election in the involved region. Members in the involved region use their regional views to discover regional membership information and the member with the smallest id announces itself as a new leader in the region by broadcasting a message "I-am-a-new-leader" including its id and location information. The members in the region receive that beacon and update the information for a regional leader in their regional view.

4 Performance Model

We develop a performance model to evaluate the communication cost for group key management in the proposed region-based protocol and to find the optimal regional size to minimize the communication cost. The traditional key agreement protocol is also considered in the paper as a special case in which all members are located in one region. We apply a hexagonal coverage model to represent a geographical area. Figure 3 shows a case in which a geographical area of πr^2 is approximated by $3n^2 + 3n + 1 = 37$ regions with n=3. Conceivably, the same geographical area can also be divided into 19 and 7 larger regions with n=2, and 1, respectively. How many regions to divide a geographical area into in order to minimize the communication cost for group key

management is a problem we aim to solve. A hexagon here represents a region. A member can move around by crossing boundaries between regions. Assuming that members are always confined in the geographical area of πr^2 as in a battlefield situation, it is easy to see that, $P_{RM}(n)$, the probability that a member moves across a boundary between two regions once a move is made, is given by:

$$P_{RM}(n) = \frac{6(3n^2+3n+1)-(12n+6)}{6(3n^2+3n+1)} \quad (1)$$

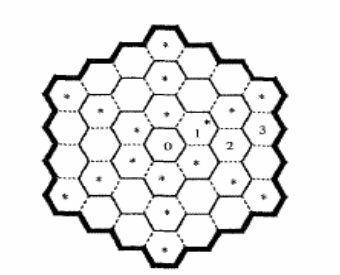

Figure 3: A Geographic Area Divided into 37 Regions with $n = 3$ based on Hexagonal Coverage Model.

Let the regional mobility rate of a member with respect to the original geographical area (i.e., one large hexagonal region only) be σ. As we divide the area into more regions (i.e., from 1, 7 to 19, and so on as we increase n from 0, 1 to 2), the regional mobility increases since the regional size decreases. Thus, as a group has more regions, we expect to have more boundary crossing events induced by mobility of members. We calculate the regional mobility rate σ_n, that is how often a regional boundary crossing event occurs as a function of n, as follows:

$$\begin{array}{lll} level\ 0 & 1\ hexagon & \sigma_0 = \sigma \\ level\ 1 & 7\ hexagons & \sigma_1 = 3\sigma P_{RM}(1) \\ level\ 2 & 19\ hexagons & \sigma_2 = 5\sigma P_{RM}(2) \\ \vdots & \vdots & \vdots \\ level\ n & (3n^2+3n+1)\ hexagons & \sigma_n = (2n+1)\sigma P_{RM}(n) \end{array} \quad (2)$$

For member population, we consider that members in a group are randomly distributed according to a homogeneous spatial Poisson process with density λ_p. Thus, for a geographical area with size $A = \pi r^2$, the average population of the group, N, is calculated as:

$$N = \lambda_p \times A \quad (3)$$

The number of regions, $R(n)$, is a function of n given as follows:

$$R(n) = 3n^2 + 3n + 1 \quad (4)$$

Thus the average number of members in a region, $N_R(n)$, is given by:

$$N_R(n) = \lambda_p \times \frac{A}{R(n)} \quad (5)$$

Our performance metric used for measuring the proposed group key management protocol is based on the *total communication cost per unit time* incurred in response to group key management events including regional mobility induced, group join/leave, and periodic beaconing events. Thus, the total communication cost consists of three components:

- *Regional Mobility Cost* – $C_{mobility}$: this is the cost in response to mobility-induced regional boundary crossing events.
- *Group Join/Leave Cost* – $C_{join/leave}$: this is the cost for handing group join or leave events. This cost also includes the cost caused by connection/disconnection events by group members.
- *Periodic Beaconing Cost* – C_{beacon}: this is the cost for maintaining view consistency by all members through periodic beaconing. Thus, this cost includes the cost for broadcasting periodic beaconing messages such as "I-am-alive," "I-am-a-new-leader," etc. By using this mechanism, member connection or disconnection events can be detected.

As a result, the total communication cost is calculated by:

$$C_{total} = C_{mobility} + C_{join/leave} + C_{beacon} \quad (6)$$

4.1 Cost for Regional Boundary Crossing: $C_{mobility}$

This cost includes two cases, that is, boundary crossing by non-leaders and by leaders. Thus, $C_{mobility}$ is given by:

$$C_{mobility} = \Lambda_m \times \left[C_{mobility}^{non-leader} + C_{mobility}^{leader} \right] \quad (7)$$

Here $\Lambda_m = \sigma_n \times N$ is the aggregate regional mobility by all members in the system. The cost for the system to handle a non-leader member crossing a regional boundary is:

$$C_{mobility}^{non-leader} = P_{non-leader} \times \left[C_{intra} \times 2 \right] \quad (8)$$

Here $P_{non\text{-}leader}$ is the probability of a non-leader given by $P_{non\text{-}leader} = (N - N_{leader})/N$ where N is the total number of members in the group and N_{leader} is the number of leaders in the group. C_{intra} is the cost incurred for rekeying K_R and updating the regional view in a region, as given in Equation (11) below. On the other hand, the cost for handling a leader member boundary crossing event is:

$$C_{mobility}^{leader} = P_{leader} \times \left[C_{intra} \times 2 + C_{inter} + C_{leader}^{change} \right] \quad (9)$$

where C_{inter} is the cost for rekeying a leader key and updating the leader view, as given below in Equation (13), $P_{leader} = N_{leader}/N$ where $P_{leader} = 1 - P_{non\text{-}leader}$ is the

probability of a leader crossing a regional boundary, and C_{leader}^{change} is the cost for changing a leader in a region, given below in Equation (15). Summarizing above, $C_{mobility}$ is given by:

$$C_{mobility} = \Lambda_m \times \left\{ \left[2 \times C_{intra} \right] + P_{leader} \times \left[C_{inter} + C_{leader}^{change} \right] \right\} \quad (10)$$

The cost for intra regional communications (C_{intra}) in a region can be calculated by:

$$C_{intra} = \left[C_{update}^{intra} + C_{rekey}^{intra} \right] \times H_{region} \quad (11)$$

where C_{update}^{intra} is the cost for updating a regional view, C_{rekey}^{intra} is the cost for rekeying a regional key, and H_{region} is the number of hops within a region for a regional leader to disseminate a regional view or key to the members in its region, given by:

$$H_{region} = \frac{s}{R} \qquad s = \sqrt{\frac{2}{3\sqrt{3}} A_{region}} \quad (12)$$

$$A_{region} = \frac{A}{N_R(n)}$$

Here A_{region} is the area of a hexagonal region based on n, $N_R(n)$ is the number of regions as given in Equation (5), s is the side length of a hexagonal region that is the same as the circum-radius of a hexagonal region, and R is the per-hop radio range.

The cost for inter regional communications (C_{inter}) is computed as:

$$C_{inter} = \left[C_{update}^{inter} + C_{rekey}^{inter} \right] \times H_{leader} \quad (13)$$

where C_{update}^{inter} is the cost for updating the leader view, C_{rekey}^{inter} is the cost for rekeying the leader key, and H_{leader} is the number of hops among leaders for a leader to disseminate a leader view or key to other leaders, given by:

$$H_{leader} = \frac{r}{R} \quad (14)$$

For C_{leader}^{change}, the outgoing leader would broadcast two messages showing its leaving intention to its regional members using its regional key and to other leaders using a leader key respectively. In addition, the new leader would broadcast two messages expressing "I-am-a-new-leader" to its regional members and to leader group using its regional key and a leader key respectively. Further, these messages need to travel through a number of hops at the leader and intra-regional levels reflected by H_{leader} and H_{region} respectively. Thus, the cost C_{leader}^{change} for a leader change is calculated as:

$$C_{leader}^{change} = H_{leader} \times \left[M_{old-leader}^{leaders} + M_{new-leader}^{leaders} \right] + H_{region} \times \left[M_{old-leader}^{regional-members} + M_{new-leader}^{regional-members} \right] \quad (15)$$

4.2 Cost for Group Join/Leave: $C_{join/leave}$

$C_{join/leave}$ includes the cost for handling group join and leave. Thus,

$$C_{join/leave} = \Lambda_J \times C_{join} + \Lambda_L \times C_{leave} \quad (16)$$

Here Λ_J and Λ_L are the overall group join and leave rates of all members, respectively, given in Equation (24) below. A group join event requires the update of the regional view and the rekeying of the regional key in the region from which the join event is originated, the cost of which is C_{intra}, as well as the update of the group view and the rekeying of the group key, the cost of which is C_{group}. Therefore,

$$C_{join} = C_{intra} + C_{group} \quad (17)$$

where C_{group} is given by:

$$C_{group} = C_{update}^{group} + C_{rekey}^{group} = \left[H_{leader} \times M_{update}^{leaders} + H_{region} \times N_{region} \times M_{update}^{regional-members} \right] + \left[H_{region} \times N_{region} \times M_{rekey}^{regional-members} \right] \quad (18)$$

Here $M_{update}^{leaders}$ is the number of bits required in a broadcast message for updating the group view for the leaders, $M_{update}^{regional\text{-}members}$ for updating the group view for members in a region, and $M_{rekey}^{regional\text{-}members}$ for rekeying the group key for members in a region. Also N_{region} is the number of regions in the group.

The cost for group leave event includes two cases, namely, when a non-leader member leaves and when a leader leaves the group. Thus the cost for a group leave event is:

$$C_{leave} = C_{leave}^{non-leader} + C_{leave}^{leader} \quad (19)$$

with

$$C_{leave}^{non-leader} = P_{non-leader} \times \left[C_{intra} + C_{group} \right] \quad (20)$$

$$C_{leave}^{leader} = P_{leader} \times \left[C_{intra} + C_{inter} + C_{group} + C_{leader}^{change} \right] \quad (21)$$

where C_{intra}, C_{inter}, C_{group}, and C_{leader}^{change} are given earlier in Equation (11), (13), (18) , and (15) respectively, and P_{leader} and $P_{non\text{-}leader}$ are as previously described.

4.3 Cost for Periodic Beaconing: C_{beacon}

C_{beacon} includes the cost of beaconing messages in two levels, namely, intra-regional beaconing among members in a region for maintaining the regional view, and inter-regional beaconing among leaders for maintaining the leader view. Thus, C_{beacon} is computed as:

$$C_{beacon} = \left[\Lambda_{RB} \times M_{alive} \times H_{region}\right] + \left[\Lambda_{LB} \times M_{alive} \times H_{leader}\right] \quad (22)$$

where M_{alive} is the number of bits in a beacon message, and Λ_{RB} and Λ_{LB} are the overall beacon rates by all the members at the intra-regional level, and by all the leaders at the inter-regional level, respectively. Λ_{RB} and Λ_{LB} are obtained from the reciprocals of the periodic beaconing intervals, T_{RB} and T_{LB}, at the intra-regional level and at the leader level, respectively, multiplied by the number of members, N, and the number of leaders, $N_{leaders}$ (equal to N_{region}), in the group, respectively, i.e.,

$$\Lambda_{RB} = N \times \frac{1}{T_{RB}} \qquad \Lambda_{LB} = N_{leader} \times \frac{1}{T_{LB}} \quad (23)$$

5 Numerical Example

We exemplify the proposed region-based group key management protocol and the performance model developed by the use of a well-known CKA protocol, namely, Group Diffie-Hellman (GDH) [8], at the intra-regional and inter-regional levels, to illustrate the tradeoff between the cost involved in group key management and the regional size. The extreme case of having just one region to accommodate all group members is the traditional non-region-based group key management protocol, which we use as a baseline case for performance comparison. We demonstrate that the overall cost for group key management is sensitive to several identified model parameters, including the regional size. In particular, there exists an optimal regional size that will minimize the overall cost. Table 2 below gives basic model parameters while Table 3 gives parameters derived from basic parameters.

Parameter	Meaning
N	Number of nodes in a group
σ	Mobility rate per node
λ	Group join rate per node
μ	Group leave rate per node
λ_p	Population density
A	Operation area of the mobile group. $A = \pi r^2$ (unit is km^2) where r is the radius
R	Per-hop radio range
k	Size (number of bits) of a group key
v	Size of each intermediate value in CKA
T_{RB}	Intra-regional beaconing interval
T_{LB}	Inter-regional beaconing interval
M_{alive}	Size of a beacon message
U_{view}	Size of an update message

Table 2: Basic Model Parameters.

Parameter	Meaning
σ_n	Regional mobility rate per node
Λ_J	Aggregate group join rate
Λ_L	Aggregate group leave rate
Λ_{RB}	Aggregate periodic beaconing rate from all the members in a region
Λ_{LB}	Aggregate periodic beaconing rate from all the leaders in the group

Table 3: Derived Parameters.

5.1 Parameterization

We first parameterize the model (that is, give values to model parameters) based on the basic set of parameters given in Table 2. The aggregate join and leave rates, Λ_J and Λ_L, can be derived by considering a two-state machine as shown in Figure 4 in which state G (Group) means that a member is in the group while state NG (Not-Group) means that it isn't. When the state is NG, the member can join the group with rate λ and conversely when the state is G, the member can leave the group with rate μ. Consequently, the probability that a member is in states G and NG are $P_G = \lambda/(\lambda+\mu)$ and $P_{NG} = \mu/(\lambda+\mu)$, respectively. Since there are N nodes in the group, the aggregate rates for group join and leave, Λ_J and Λ_L, are given by:

$$\Lambda_J = \lambda \times N \times \frac{\mu}{(\lambda+\mu)} \qquad \Lambda_L = \mu \times N \times \frac{\lambda}{(\lambda+\mu)} \quad (24)$$

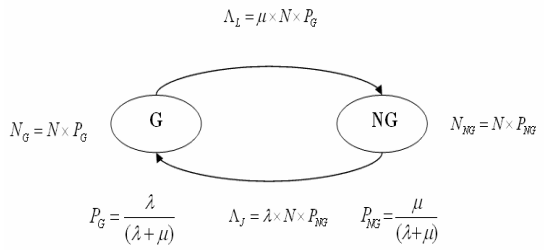

Figure 4: Two-State Machine for Join/Leave Process.

We exemplify our region-based key agreement protocol with GDH [8] as the CKA protocol in this work. Particularly, we adopt GDH.3 in [8] since it is a well known efficient and robust protocol using 2-party Diffie-Hellman protocol. Below we briefly explain how GDH works to parameterize the communication cost involved to agree on a new key as a function of member size, m.

The GDF.3 protocol is comprised of four stages. The first stage shows the process of collecting contributions from all group members. For example, M_1 raises α to the power of N_1, performing one exponential computation generating α^{N_1}, M_2 computes $\alpha^{N_1 N_2}$ by raising α^{N_1} to the power of N_2, and so on until M_{m-1} computes $\alpha^{N_1 \ldots N_{m-1}}$.

Thus after processing the upflow message, M_{m-1} obtains $\alpha^{\Pi\{N_k \mid k \in [1, m-1]\}}$ and broadcasts this value in the second stage to all other participants. At this time, every M_i factors out its own exponent and forwards the result to M_m. In the final stage, M_m collects all inputs from the previous stage, raises every one of them to the power of N_m and broadcasts the resulting m-1 values to the rest of the group. Every M_i has a value of the form $\alpha^{\Pi\{N_k \mid k \in [1, m-1] \wedge k \neq i\}}$ and can easily generate the intended group key K_m. This GDH protocol (GDH.3) has two appealing characteristics. One is that it has constant message sizes. The other is that the protocol has a constant (and small) number of exponentiations for each M_i (except for M_m with m exponentiations required).

Stage 1: *upflow*	$M_1 \quad M_2 \quad \ldots \quad M_{m-2} \quad M_{m-1}$	
message size	$v \quad v \quad \ldots \ldots \quad v$	$= v(m-2)$
Stage 2: *broadcast*	$M_{m-1} \quad M_i$ *where* $i \neq m$-1	
message size	v	$= v$
Stage 3: *response*	M_i *where* $i \neq m \quad M_m$	
message size	v *from each* M_i	$= v(m-1)$
Stage 4: *broadcast*	$M_m \quad M_i$ *where* $i \neq m$	
message size	$v(m-1)$ *intermediate values*	$= v(m-1)$
Total communication cost		$= 3v(m-1)$

Figure 5: Communication Overhead for GDH.

Figure 5 summarizes the total communication cost incurred when GDH is invoked to generate a new key, computed as $3v(m-1)$, where m is the number of nodes and v is the size of each intermediate value. This cost is used to parameterize C_{rekey}^{intra} for rekeying a regional key and C_{rekey}^{inter} for rekeying the leader key, as a function of the number of nodes (m) involved with the rekeying process, which in turn depends on the regional size.

5.2 Numerical Analysis

Parameter	Default Value
σ	1/(60*60*2)
λ	1/600 (once per 10 minutes)
μ	1/6000 (once per 100 minutes)
λ_p	10 *nodes/km*^{2}
A	25 π *km*^{2}
R	100m
k	64 bits
v	64 bits
T_{RB}	5 seconds
T_{LB}	2 seconds
U_{view}	500 bits

Table 4: Default Parameter Values.

Below we report numeric data for the communication cost incurred in executing the proposed region-based group key management protocol as a function of model parameters. We demonstrate that there exists an optimal regional size that minimizes the overall communication cost. The effect of regional size is represented by a parameter, n, where n=0 means that there is only one region, n=1 means 7 regions, n=2 means 19 regions, and so on. (Note that this parameter n computes the number of regions based on Equation (4).)

We evaluate the effect of n on the overall communication cost rate (C_{total}) given in Equation (6) while varying other critical parameters to test their effects. Table 4 shows the default parameter values used in this case study.

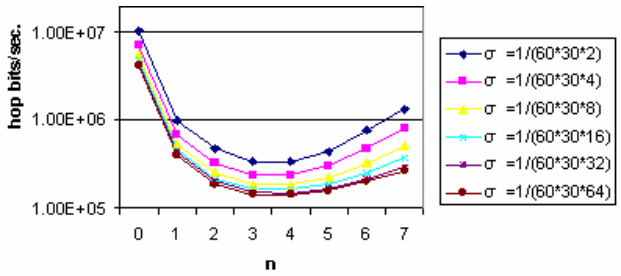

Figure 6: Overall Cost (C_{total}) vs. n as a Function of σ.

Figure 6 shows the effect of n on the communication cost rate (C_{total}) with the per-node mobility rate (σ) varying. As the size of a region decreases (as n increases), C_{total} increases until it reaches the optimal point (at n = 3 for the first three curves and n = 4 for the last three curves) that would minimize C_{total}, after which C_{total} increases again beyond that point. Note that a larger n indicates there are more regions and consequently there are fewer members in a region. The reason that an optimal n exists is that as n increases, the inter-regional overhead (i.e. updating and rekeying cost at a leader level) increases while the intra-regional overhead (i.e. updating and rekeying cost at a regional level) decreases. Initially, the total communication cost decreases as the number of regions increases because of the decreasing intra-regional overhead while it increases again after the optimal n reaches because of the increasing inter-regional overhead as n increases. It is worth noting that the special case in which there is only one region (when n=0) performs badly compared with when there are more regions, especially when the number of members is large. Further, we note that the optimal n identified decreases as σ increases because as n increases the overall regional mobility rate also increases as a result of more regions being in the system, thus increasing the cost associated with mobility manegement. Consequently the system favors fewer regions (a lower n) as σ increases.

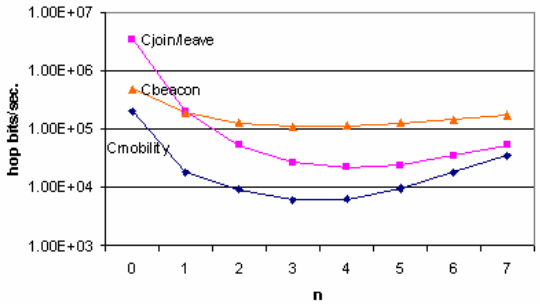

Figure 7: Breakdown of $C_{mobility}$, $C_{join/leave}$, C_{beacon} vs. n.

Figure 7 breaks down the overall cost into its constituents $C_{mobility}$, $C_{join/leave}$, and C_{beacon} as a function of n for the case in which $\sigma = 1/(60*30*64)$ to illustrate why an optimal value $n = 4$ is obtained. We see in this case $C_{join/leave}$ dominates all others and the optimal point is at $n = 4$ to balance the intra-regional and inter-regional costs for join/leave operations.

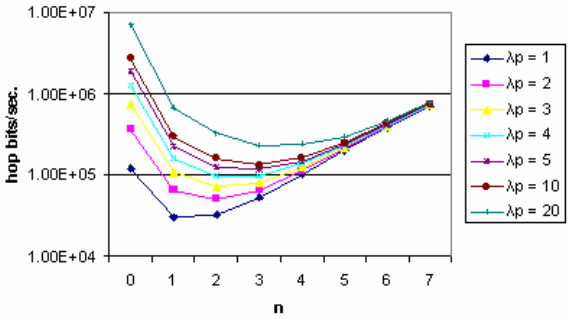

Figure 8: Overall Cost (C_{total}) vs. n as a Function of λ_p.

Figure 8 shows the effect of population densities (λ_p) on C_{total}. First, as λ_p increases, C_{total} increases because of the increased number of members in each region, thus introducing a higher intra-regional cost for updating the regional view and rekeying the regional key. Here it should be noted that since the number of leaders remains a constant under different λ_p, C_{total} increases as λ_p increases due to the increased intra-regional overhead. Second, we observe that the optimal n shifts to the right as λ_p increases. That is, a smaller λ_p produces a smaller optimal n (e.g.. optimal $n = 1$ at $\lambda_p = 1$) while a larger λ_p generates a larger optimal n (e.g., optimal $n = 3$ at $\lambda_p = 20$). This is so because the intra-regional cost always favors fewer members in a region and thus a small regional size is favored under high λ_p and conversely a large regional size is preferred under low λ_p. Lastly, we also notice that as n increases, C_{total} converges to almost the same point, as C_{total} at $n = 7$ exemplifies. This is because in the extreme case where there are a lot of regions, there is little intra regional overhead and inter-regional dominates, thus causing C_{total} to be at a high n.

6 Conclusion

In this paper, we have proposed and analyzed a scalable and efficient region-based secure group key management protocol to support secure group communications in mobile ad hoc networks. By using a region-based hierarchical key management technique, the proposed group key management protocol not only reduces network communication costs, but also provides robust security properties. We discovered that there exists an optimal regional size that would minimize the overall network communication cost when given a set of parameter values characterizing the operational condition. The existence of the optimal regional size is a tradeoff between inter-regional and intra-regional overheads and it is sensitive to certain identified system parameters such as the node population density, node mobility rate, and the group join/leave rate in our case study. In the future, we plan to extend the protocol to consider group partitioning and merging in mobile ad hoc networks, as well consider energy consumption as a performance metric. Lastly, the protocol coupled with authentication can only deal with outsider attacks. We plan to extend the protocol to consider insider attacks and intrusion detection.

Acknowledgement

This research work was supported by a National Science Foundation IGERT grant #9987586.

References

[1] Y. Amir, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G. Tsudik, "Secure Spread: An Integrated Architecture for Secure Group Communication," *IEEE Transactions on Dependable and Secure Computing,* Vol. 2, No. 3, 2005, pp. 248-261.

[2] Y. Amir, Y. Kim, C. Nita-Rotaru, G. Tsudik, "On the performance of group key agreement protocols," *ACM Transactions on Information and System Security*, Vol. 7, No. 3, 2004. pp. 457-488.

[3] Y. Amir, et al., "Secure group communication using robust contributory key agreement" *IEEE Trans. on Parallel and Distributed Systems,* Vol. 15, No. 5, 2004, pp.468-480.

[4] Y. Kim, A. Perrig, and G. Tsudik, "Tree-based Group Key Agreement," *ACM Transactions on Information and System Security,* Vol 7, No. 1, 2004, pp. 60-96.

[5] Y. Kim. A. Perrig and G. Tsudik, "Communication-Efficient Group Key Agreement," *IFIP TC11 16th Annual Working Conference on Information Security*, " June 2001, pp. 229-244.

[6] X.S. Li, Y.R. Yang, M.G. Gouda, S.S. Lam, "Batch Rekeying for Secure Group Communications," 10th *International World Wide Web Conference on World Wide Web*, 2001.

[7] O. Rodeh, K. Birman, and D. Dolev, "Using AVL Trees for Fault Tolerant Group Key Management," Cornell University, Computer Science, Technical Report 2000-45, 2000.

[8] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-Hellman Key Distribution Extended to Group Communication," *3rd ACM Conf. on Computer and Communications Security*, January 1996.

[9] J.W. Wilson and I.R. Chen, "Performance analysis of location-based group membership and data consistency algorithms in mobile ad hoc networks," *International Journal of Wireless and Mobile Computing,* 2005.

[10] C. Zhang, B. DeCleene, J. Kurose, D. Towsley, "Comparison of Inter-Area Rekeying Algorithms for Secure Wireless Group Communications," *Performance Evaluation.* Vol. 49, No. 1-4, 2002, pp. 1-20.