AN ADAPTIVE SCHEME TO MANAGE MOBILITY FOR SECURE MULTICASTING IN WIRELESS LOCAL AREA NETWORKS

by

Sriram Cherukuri

A Thesis Presented in Partial Fulfillment
of the Requirements for the Degree
Master of Science

ARIZONA STATE UNIVERSITY

May 2004

AN ADAPTIVE SCHEME TO MANAGE MOBILITY FOR SECURE MULTICASTING IN WIRELESS LOCAL AREA NETWORKS

by

Sriram Cherukuri

has been approved

January 2004

APPROVED:

_____, Chair

_____

_____

Supervisory Committee

ACCEPTED:

_____

Department Chair

_____

Dean, Graduate College

ABSTRACT

Multicasting in wireless networks such as wireless local area networks (LANs) is a very significant communication paradigm. Wireless networks are characterized by stringent constraints due to mobility of hosts, scarcity of energy, and wireless bandwidth. In such situations, multicasting offers solutions which are efficient. Security is very important for multicast services. As in any other communication paradigm, the data in multicast communication must be secure. Security features like secrecy, authenticity, and freshness can be achieved by means of cryptographic techniques. Access control to multicast services is very important since unauthorized access poses a huge problem in wireless networks. Access control can be handled in an approach different from cryptographic techniques. In this approach, the location of the requestor is used as the input factor to determine whether access is to be granted or not. Location-based Access Control (LBAC) is more scalable and superior in terms of user privacy. But providing LBAC in mobile wireless networks with a high degree of mobility is non-trivial. In this thesis, three schemes for secure multicasting incorporating Location-based Access Control are presented. The three schemes vary according to whether the base station shares the same session key (SSK) with all the members of its cell or has a different session key (DSK) for each one of the members, or has a combination (Hybrid) of the two schemes for efficient key management. Mathematical analysis and simulations to show that the hybrid adaptive scheme performs better than the other two schemes at high mobilities are presented.

Dedicated To my Mother

ACKNOWLEDGMENTS

I would like to thank Dr. Sandeep Gupta for his constant support and encouragement without which this work would not have been possible.

I am thankful to Dr. Arunabha Sen and Dr. Partha Dasgupta for sparing their valuable time to be part of the committee.

This research work has been partially funded by NSF grants ANI-00196156, ANI-0086020, ANI-0123980 and DGE-9870720.

TABLE OF CONTENTS

Page

Page

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Wireless Local Area Networks are proliferating at a very fast rate. When compared to the conventional wired networks, a wireless local area network offers significant advantages. A wireless local area network allows users to move about in a network area and connect to the network via different access points. Typical scenarios include university campuses and offices. A user can connect to the network and access services from different locations such as conference venues, class rooms and so on. This feature is referred to as mobility. Mobility is one of the most important issues when it comes to both the advantages it provides and the research challenges it poses. In addition, there are many scenarios where it may not be possible to lay cables extensively which is required for a wired local area network. Historical buildings of archeological importance are not amenable to such cable laying. In such scenarios a wireless local are network offers a suitable solution with minimal cable laying, thereby requiring least alterations to the building. The cost of installing a wired Local Area Network increases with the numbers of users, which is not the case with wireless Local Area Networks. Wireless Local Area networks also offer a economic solution to temporary scenarios like conference venues where the requirement is not permanent.

1.1. Constraints of Wireless Networks

Wireless devices are severely constrained in terms of resources, when compared to the traditional computing devices like desktop computers. Most of these constraints arise from the required characteristics of wireless devices like wireless communication, mobility and so on. Most of the wireless device will be mobile. This places a severe restriction on their size. The power source of these device is a battery. The aforesaid restriction on size restrict the size of the battery and in turn the capacity of the battery of the device. The option of supplying power by means of wires is totally ruled out due to the mobility requirements. Hence the wireless devices have very low power compared to their wired counterparts. The wireless devices communicate using the wireless medium. The bandwidth associated with the wireless medium is typically a few orders of magnitude less than the bandwidth available in the wired networks. The wireless links are prone to errors to a greater extent. The wireless devices tend to have low computing power. This is due to low power available. The size constraints also limit the memory available. This places a tab on their ability to perform computation requiring a lot of memory. Thus algorithms cannot be computationally complex. Hence while designing protocols and architectures for wireless systems such as wireless Local Area Networks the above constraints have to be kept in mind in order to achieve efficient performance.

1.2. Multicast Applications

Group oriented services are gaining popularity at a very fast rate. Group communication involves the delivery of data or services to multiple users. This kind of services are becoming very important in wireless Local Area Networks. There are a multitude of applications possible with such services due to the presence of a large number of users requiring the same set of services in a wireless Local Area Network. The possible applications include stock market applications, warehouse monitoring, and other collaborative work. Multicasting provides an important mode

of communication for such group oriented services. Multicasting involves the distribution of the same data or service to multiple receivers. The sender along with the receivers form the multicast group. Multicast is significant in wireless networks since it can be achieved by a single transmission to the relevant multicast address rather than performing multiple unicast transmissions to all the receivers of the multicast group after replicating the data. This is possible due to the nature of the of the wireless medium wherein all the nodes in the transmission range of the sender receive the transmitted signal. Multicasting enables significant saving in the energy consumed as multiple transmissions and in turn multiple receptions are avoided. Multicasting also saves a lot of bandwidth due to channel re-use. Hence multicasting in wireless Local Area Networks with scarce energy and bandwidth is an attractive proposition.

1.3. Secure Multicasting

It has been mentioned earlier that multicasting has numerous applications. Many application are designed to operate in the open, that is they do not require security. But there are also many application which require security inherently. These applications might be dependent of security for their very existence. Multicast communication is subject to security vulnerabilities similar to unicast communication. Thus a multicast communication is susceptible to threats ranging from passive eavesdropping to active data modification. We discuss the security requirements corresponding to various threat in detail in section 2.6 of chapter 2. Various multicast applications in wireless LANS require varying degrees of security. Some applications are discussed here to elaborate the need for securing multicast services in wireless Local Area Networks.

In a university campus settings, there are resources which are provided by the university. The users include students and university staff. These people will use a multitude of mobile devices to access these services. It is undesirable that people who are not supposed to be accessing the resources (such as passers by) access the resources. Also within the legitimate users access may

have to be controlled based on some other conditions. In a hospital, the information about specific patients is multicasted to only people who are linked to the patients. It is required that the patients' information secrecy is preserved. In each of the above applications if the multicast data is not secured it may lead to undesirable consequences ranging from loss of data to monetary losses to service provider.

When we try to come up with a scheme for secure multicasting in wireless LANs, two issues are of utmost significance; the *basic security primitives* and *efficient performance* in terms of resource consumption. A secure multicast protocol must ensure that only legitimate users are able to receive the data in useful form. To all others, even if they receive it, it should be unintelligible. Cryptographic techniques are used in order to achieve requirements of security like availability, confidentiality, integrity, authentication, and non-repudiation [14] and access control. While trying to achieve these objectives it is essential that resource consumption (such as energy and bandwidth) is kept to the minimal. In this research work the main objective is to minimize the cost incurred in terms of communication and computation, for implementing the security mechanism by using an adaptive approach to the solution. Mobility is a very significant characteristic of the mobile devices forming part of a wireless Local Area Network. Providing any service or feature in such a network involves additional overhead due to mobility. Security is no exception to this. In fact mobility introduces certain additional special requirements. In this research, we focus on managing multicast group membership dynamics arising out of the mobility prevailing in the network.

1.4. Overview of the Thesis

In this thesis, we examine the constraints and requirements of secure multicasting in wireless Local Area Networks. Then the possible solutions for secure multicasting are explored. Three possible solutions are presented. The working of the schemes are presented in detail. One of the

solutions presented is an adaptive solution. They are analyzed and their comparisons are presented. In addition to analytical comparisons, simulations are performed in Network Simulator 2 and the results are compared in order to come up with optimal solution for different scenarios.

This thesis document is organized as follows. In chapter 2 we present the preliminaries required for this research. In chapter 3 we describe related work in this area. We describe our algorithms in chapter 4. In chapters 5 and 6 we present mathematical analysis and simulation results for our schemes respectively. Finally we conclude and present the future work in chapter 7.

CHAPTER 2

PRELIMINARIES

In this chapter we describe the conceptual preliminaries that form a part of this research. The understanding of these concepts is significant as their application significantly improves the performance of the secure multicast schemes in addition to providing the framework.

2.1. Location based Access Control

In a secure multicast scheme, the group keying material has to be changed, whenever there is a change in the group membership. Specifically whenever a user enters the multicast group the new entrant is assigned a new key. Before assigning a new key the new entrant has to be authenticated in order to provide access to the multicast data. In the existing literature for secure multicasting the authentication is achieved by means of public/private key pair [2]. This ***identity*** based solution tends to be expensive in terms of energy consumption due to the heavy computation that is involved. Hence we adopt a different approach in this research. In our model, we adopt the ***location*** of the mobile host as the criterion to define the access to multicast data. The services and the data accessed by the mobile host are dependent on its location. The location of the mobile host is used as a parameter while making a decision whether to grant access or not. This is referred to as ***location based access***. This model is similar to the Pervasive computing environment model. In Pervasive computing environments, ***location based access*** is used for controlling the access to resources in networks consisting of a large number of users with

a disparate set of characteristics. Consider a theme park scenario consisting of various rides and shows. Real time information is provided only to ticketed persons who are within the enclosure. It should not be possible for persons inside the wireless range but outside the enclosure to the information. Providing location based access involves ascertaining to a reasonable extent that the requestor is at a legitimate location. The following approaches are possible,

- ***Direct Approach:*** In this approach the user informs the base station about its location explicitly while requesting a service. The base station then checks if the location claim is true by techniques such as measuring the time delay for sending response to a nonce [13]. This method needs to address issues such as propagation delay while estimating the location. Hence this method should be used when the required location granularity is very high. This means that base station has to differentiate between small variations in locations. Cryptographic techniques are not used here.

- ***Indirect Approach:*** In this approach the base station assures itself about the user's position without the user sending its exact location information. This may achieved by using a combination of computing and physical techniques. For instance a user may be provided with a key(or token) every time it enters the legitimate area. Here the possession of a key implies presence inside the *service area*. Here the base station is not concerned with the exact location, but only whether requester is inside the service area or not [3]. While using this method the service area may not be accurately demarcated. But it is light weight and consumes less resources.

The knowledge of the user location is used to grant access to resources, but it is equally important to protect the privacy of his location. In our research work, we use the ***indirect*** method mentioned above. The user's privacy of location is not violated because the system does not possess the knowledge of the exact location, nor is his movement monitored continuously as history of exact location is not maintained. In addition not using the identity for access

control prevents the individual identity to be mapped to his access pattern. This prevents any form of profiling of the user. This is tune with privacy requirements of the pervasive computing environments

2.2. Assumptions and System Model

In the following subsections we describe the requirements of secure multicast and present a description of our problem. Before that in this subsection we describe some assumptions which we make and the system model which we use.

2.2.1. Basic Assumptions.

- We assume that all the multicast traffic originates from the base station. This assumption is made due to the fact that multicast traffic in most of the applications such as video conferencing have such a model. Moreover mobile hosts can send their traffic to the base station and it in turn multicasts it. So the the problem reduces to that of multicasting by the base station.

- A legitimate user is assigned a token as a means of authentication. This may be assigned by means of access points located only inside the service area. For this purpose techniques described in [5],[16] which involve the use of portable device carried on the users person, may be used.

- In this research work we assume the existence of the reliable protocols for multicasting [10] and unicasting [4] data messages and rekey messages.

- Appropriate Medium Access layer protocols are assumed to assure contention free channel access for communication [4].

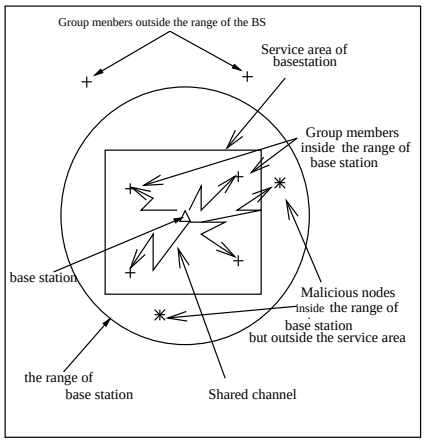

Figure 1. System Model

2.2.2. System Model. The system consists of a group of nodes, which constitute the multicast group. Each of these nodes attaches itself to a base station depending on its location. The group members keep moving in and out of a cell in random patterns. Each base station caters to a cell like a floor of a building. The cell is a part of the transmission range of the base-station. There exist areas in the range, which are not part of the cell. The base station keeps track of the membership of the cell. The members of the group periodically inform the base station of their presence. Whenever the base station detects a change in the membership of its cell, keys are distributed, depending on the protocol that is followed. The topology at a random instant of time is as shown in figure 1. With regard to the multicast data, the base station multicasts it to all the members which share the same session key, while it unicasts it to members with whom it shares unique keys. The base station expects the legitimate group members to move in and out of the cell. It also expects malicious nodes to be present in the transmission range. The security model is based on the shared key encryption.

2.3. Key Agreement and Set Up

In a secure multicast scheme, when a user U wants to join a multicast group it sends a join request to the base station B. The base station then verifies if the user can be granted access

and then assigns it a secret key. The establishment of the unique key is done by the following protocol. If the new user is legitimate, then he or she would be in position to obtain a token(or weak secret) P from an authentication point associated with the service area. The authentication point is analogous to the ticket checking at the entrance of a theater. The goal of the protocol is to enable U and B to mutually authenticate each other based on P, and agree on a strong individual key K, in such a way that an attacker watching the traffic will not be able to learn K or mount a dictionary attack on P. During the protocol, U generates random string S_u. B generates two random strings: R_b, and S_b. A suitable symmetric key encryption scheme, which is freely available and which can be used with the unique key is considered. The lengths of the other random strings is left to the specific implementation of the protocol. The protocol proceeds as follows:

1. $U \rightarrow B : X$ Hi I am U
2. $B \rightarrow U : R$ Prove it
3. $U \rightarrow B : E_P(hash(R), S_x)$
4. $B \rightarrow U : E_P(hash(S_x), S_y)$

$E_P(msg)$ refers to the encryption of msg using P as the key. In the first step the entering node U sends a message requesting a key. Upon receiving the request the base station B generates a random number R_b and sends it to U in the second step asking U to authenticate itself. In the third step, in order to authenticate itself U encrypts R_b along with a random nonce S_u using P(a weak shared secret or token). On receiving it, B decrypts it with P and if it results in R_b then U is authenticated to B. B also extracts S_u. Here S_u serves two purposes. One is that U does not have to encrypt a random number which is not generated by it. This prevents resend attacks [14]. Secondly S_u is used as a parameter to the function used to generate the unique key. In the last step B encrypts with P the combination hash of S_u and S_b, which is a random nonce

generated by B. Now U can obtain S_b. S_u and S_b, which are known to both U and B are used as parameters for the generation of the unique key. Since both the parties contribute the input material for key generation it is not possible for one of the parties to act maliciously (i.e.) select a weak key.

It may be seen that unless an adversary knows the initial shared secret it is not possible for him to attack the above key sharing protocol. If a malicious node say M tries to masquerade as U then it will fail in the third step of the protocol, since it will not be able to encrypt R_b correctly as it does not have knowledge of weak shared secret P(only those nodes that are legitimate members of the multicast group have knowledge of P). On the other hand if some node gets hold of the key request message from U of the first step and may try to masquerade as B. In such a scenario the protocol would fail in step four, since the malicious node cannot encrypt S_u generated by U correctly as it does not have knowledge of weak secret P.

2.4. Group Communication for the Key Distribution

Session keys have to be changed after every leave and join, to achieve forward and backward message secrecy. Changing a session key may be done in two ways. After a join or leave the new session key is computed and it is encrypted with unique keys of all the members and it is unicasted to the members of the group. Another way would be as follows. After a join the new session key is encrypted with the newly established unique key of the new member and sent to it. The new session key is encrypted with the old session key and is multicasted to the older members of the cell. For the leave the new session key has to be encrypted with the unique keys and sent. The old session key cannot be used, as the user that has left has knowledge of the old session key. We have performed experiments for both above methods. They are presented in chapter 6.3.6.

2.5. Periodic Batch Re-keying

The base station responds to the events of members entering and leaving the cell as they happen. But such individual rekeying would be inefficient. Suppose a series of events, which require rekeying occur in a small interval of time, then using individual rekeying requires that we rekey for each of the events. *Periodic batch rekeying* can be used to solve these problems to a large extent. In periodic batch rekeying the events requiring rekeying are collected over a period of time called ***batch interval*** and handled together at the end of the interval. This reduces the number of rekeyings. But this procedure increases the delay to access the data, because a new user has to wait longer to be accepted by multicast group and departed user stays longer. A balance is maintained by choosing the right value for the *batch interval* (i.e.) it should not be too large nor too small[17].

2.6. Security Requirements

We conclude this chapter by describing the security requirements of secure multicast communication. A scheme for secure multicast has to satisfy the following requirements,

- ***Confidentiality:*** The communication between the base station and the users should be secret. It implies that it should be possible for an eavesdropper to extract the contents of the communication.
- ***Integrity:*** It should not be possible for a malicious entity to modify a multicast message and be passed of undetected.
- ***Authenticity:*** Authenticity ensures that the base station is sure that it is indeed communicating with a legitimate entity.
- ***Forward Message Secrecy:*** When a user leaves the multicast group, then the protocol must ensure that this user in not able to access the multicast communication occurring after

it left. This security requirement necessitates that the session key shared by that multicast group be changed when a user leaves the group. If the key is not changed then the departing member will still be able to access the multicast data after departure.

- ***Backward Message Secrecy:*** When a user enters the multicast group, then the protocol must ensure that this user in not able to access the multicast communication which occurred before it entered the group. This requirement like the previous one necessitates a change in the session key in vogue. If the existing key itself is revealed to the entering user then it might be possible for the user to gain knowledge of earlier communication by using this key.

CHAPTER 3

RELATED WORK

In this chapter we provide a description of the related work in secure multicasting. These papers express the issues and requirements of secure multicast. They also present many of the basic ideas which we use in this research. These concepts are explained in detail in chapter 2.

In [1] the author Bharghavan has proposed an elaborate scheme for secure communication in wireless Local Area Networks. The scheme presented in the paper is described briefly as follows. The main concern in this paper is to secure the final hop of the communication between the base station and the mobile host. The architecture consists of a set of mobile hosts, base stations and home computers. The base stations and the home computers are fixed computers to which the mobile hosts connect for various purposes. Every mobile host is associated with a home computer. It connects to the base station of the area in which it is present to obtain services. It is assumed that the mobile hosts share a secret key with their home computers and the home computers share a secret key with the base stations. The home computer is used as an intermediary authority to establish a secret key between the mobile host and the base station. The author suggests that this scheme can be extended to multicast by providing the legitimate mobile node with the base stations' public key. In the above scheme the multicast group dynamics due to node mobility has not been considered. The security requirements associated with group communications such as forward message security and backward message security have not been addressed. The scheme uses public key cryptography to a significant extent which would prove to be expensive. Finally

the architecture presented may not be suitable for temporary scenarios like conference venues where extensive infrastructure may not be available.

In [12] Mitra examines the differences in the security requirements of unicast and multicast communications such as key management issues arising out of group dynamics. They present the notion of secure multicast to be consisting of blocks of time. An entity may or may not be allowed to participate in the multicast during the various blocks. The entities should be allowed only if they have the relevant permission to do so. The multicast blocks mentioned earlier correspond to changes in the multicast group membership (i.e.) each block lies between two consecutive joins or leaves. The group keying material which is referred to as security associations has to be changed for every multicast a.k.a for every change in group membership. The architecture consists of Secure distribution tree consisting of secure multicast subgroups arranged in a hierarchical manner. The individual subgroups have their own keying material. Thus whenever a new member enters the groups it does so by joining a subgroup and when a member leaves it does so by leaving a subgroup. Thus only the key material of the subgroup needs to be changed. A single secure multicast group is created from the subgroups by using entities designated as the group security controller(GSC) and the group security intermediary(GSI). The GSCs are responsible for the overall security of the group. The GSA acts as a proxy for the GSI in the subgroup. The GSIs are the links between the subgroups receiving multicast data and remulticasting it within its subgroup. The Iolus key management operation is characterized by start up, joins, and leaves. The start up phase involves the actual set up of the secure multicast involving the provision of access control list(ACL). All the GSIs are started at this phase. To join the secure group a user locates its GSA and sends a join request. If the request is acceptable (based on the ACL) then the GSA establishes a secret key $K_{GSA-MBR}$ with the new entrant. Then a new group key is computed and encrypted with the existing group key and sent to the existing members. The individual key is used to send the new group key to new entrant. The joins have time out and hence have to be refreshed. The leaves

involve an entity leaving the group and a new group key is established which is sent individually to other group members securely.

In [17] the authors address the problem of managing the keys in group communication. They propose a key management architecture in which the users are divided into groups. Each of the user is provided with multiple keys. These include the whole group key, the subgroup keys, the individual keys. A secure group is a triple (U,K,R), where U is the set of users, and K is set of keys, and $R \subset \times U, K$, is a binary relation between U and K such that user u has a key k only if (u, k) is in R. The system is represented as a key graph consisting of two types of nodes namely the users and the keys used by the network. When a user leaves a secure group (U,K,R) all the keys that were held(or shared) by that particular user have to be changed. The new keys should be established securely. In order to achieve this, keys known only to the remaining users and not to the departed user have to be used. The efficiency is maximum when the number of such keys is kept to a minimum. This turns out to be an NP-complete problem. When a user enters a group it is placed in the graph and assigned a new individual key. In addition all the keys corresponding to node from entering user node to the root are rekeyed and distributed to the relevant users including the new entrant. The authors propose schemes to minimize the number of encryptions and the number of messages sent. These schemes are either user oriented or key oriented or group oriented.

In [2] the authors identify the issues in designing a secure multicast scheme for mobile wireless networks. Then they propose schemes for secure multicasting for three possible scenarios. They are non-trusted systems, semi-trusted systems and fully trusted systems. They differ based on the level to which the mobile service station(or base stations) are trusted. In the non-trusted MSS scenarios a centralized tree based algorithm is used for the entire set of mobile nodes. Each mobile host has to manage $logN$ keys which imposes a high overhead. In the case of semi-trusted MSSs the traffic is first encrypted using the session key, the session key is encrypted using the

traffic key and sent to the MSS by the Group Monitor(GM). The MSS in turn encrypts it using a cell specific key and sends to the mobile host. The mobile host has knowledge of both the cell specific key and the traffic key unlike the MSS which knows only the cell specific key. Hence only the mobile host can access data. Within the cell a tree based key management scheme such as [15]is used. In case of fully trusted MSSs the base station knows the traffic key and it decrypts the data and then encrypts it using the cell specific key. This reduces the computation at the mobile host. The group monitor and MSSs implement centralized key management. At the cell level again a centralized tree based key management is used. They describe algorithms for handling joins, leaves, handoff between cells to achieve forward message secrecy and backward message secrecy for the three scenarios.

A common aspect in all the above solutions is that the multicast group is further divided into subgroups to achieve scalability when rekeying is done since the effect of change in group membership is reduced to the subgroup. In this paper we adopt a similar approach by grouping the group members. But further we present a mechanism for grouping the member in order to minimize the rekeying overhead.

CHAPTER 4

ALGORITHMS

In this chapter we present a description of the schemes for secure multicasting. Each one of the scheme consists of algorithms for managing the keys to adjust to changes in the multicast group membership due to ***joins*** and ***leaves***. In addition to key management algorithms, each scheme also includes the multicast data transmission technique. We describe the notation used in the algorithms in the Table 1.

4.1. Single Session Key

- *Set Up*

  The multicast group is set up by the base station. The base station is provided with information(the set of legal tokens) to enable it to authenticate the legitimate users. Tokens from this set are assigned to users when then they enter the service area and are discarded when the corresponding user moves out.

- *Join*

  When a new user enters the service area he first obtains a token from the access point. The users indicate their presence to the base station by sending a beacon message. Then the base station checks if the user is already present. If not, then the beacon initiates the *iKey()*

Table 1. Notation used in Algorithms

Variable/Function	Description
U_i	User with user id i.
B	Base station.
K_s	Session key for multicasting.
$K_s^{'}$	New session key to replace existing the one.
K_i	The individual key shared by the base station and user i.
t_i^u	Time elapsed since user i sent an *update* beacon indicating its presence.
t_i^s	The time that has elapsed since the user i was first stabilized.
$groupId$	The common multicast group address.
$E_K(msg)$	The symmetric encryption of message msg with key K.
$getKey()$	Function generates a new session key and returns it.
$ikey()$	Establishes a individual key between the user and base station as described in chapter 2.
$addToList(i)$	Adds the user i to member list of base station.
$getNodeId(b)$	Returns the node Id from the beacon message b.
$isPresent(i)$	Scans the members list and returns *true* if user i is present.
$hasDeparted()$	Scans the member list of the base station and returns *true* if a user has departed.
$stableDeparted()$	Scans the member list of the base station and returns *true* if a stable user has departed.
$stabilize()$	Reclassifies users who have stayed inside the network for sufficient time(t_{stable}).
$stableList$	List of node classified as stable.
$unstableList$	List of nodes not classified as stable.

routine. At the end of the *iKey()* routine an individual shared secret key is established between the user and the base station. Now the base station checks if the entering user is the first user to enter the group. If so then it computes a group key and encrypts it with the individual key and sends it to the entering user. If it is not the first user then a new group key is computed. It is then encrypted using the existing group key and sent to the already existing members. It is sent to the entering node by encrypting it using the individual key. Refer to algorithm 1.

Algorithm 1: The base station executes the following after receiving a beacon message from a node.

$beacon = recv()$
$i = getNodeId(beacon)$
if $(isPresent(i))$ **then**
  $t_i^u = 0$
else
  Routine *ikey()* to authenticate user i and exchange individual key K_i.
  $addToList(i)$
  $t_i^u = 0$
  $K_s^{'} = getKey()$
  $B \rightarrow groupId : E_{K_s}(K_s^{'})$
  $B \rightarrow i : E_{K_i}(K_s^{'})$
end if

- *Leave*

  When a user leaves a multicast group it is detected by the base station as it maintains soft state of the membership of the cell. On detecting that a user has left the multicast group the base station computes a new group key and encrypts it using the individual keys of the remaining users and unicasts the new group key to them. The base station also discards the token assigned to the departing user. Refer to algorithm 2.

- *Data Transmission*

  In the SSK scheme data is multicasted by encrypting it with the group session key K_s and sending it to the multicast address. Refer to algorithm 3.

Algorithm 2: The base station executes the following after detecting that a user has left.

On expiry of soft state timer.
if $(hasDeparted())$ **then**
  $K_s^{'} = getKey()$
  for all $x \in memberList$ **do**
    $B \rightarrow x : E_{K_x}(K_s^{'})$
  end for
  Restart soft state timer.
else
  Restart soft state timer.
end if

Algorithm 3: The base station sends data by encrypting it with group session key.

$B \rightarrow groupId : E_{K_s}(msg)$

4.2. Different Session Keys

- *Set Up*

  The multicast group is set up by the base station. The base station is provided with information(the set of legal tokens) to enable it to authenticate the legitimate users. Tokens from this set are assigned to users when then they enter the service area and discarded when the user leaves the group.

- *Join*

  When a new user enters the service area he first obtains a token from the access point. The users indicates his presence to the base station by sending a beacon message. Then the base station checks if the node is already present. If not then the beacon amounts to the first step of the *iKey()* routine. At the end of the *iKey()* routine an individual shared secret key is established between the user and the base station.

- *Leave*

  When a user leaves the group it is detected by the base station as it maintains a soft state. The base station just discards the individual key which it shared with that user along with

the token assigned to the departing user.

- *Data Transmission*

  Data is multicasted by the base station after encrypting it with the individual keys of the members present. This is achieved by multiple unicast communications. Refer to algorithm 4.

Algorithm 4: The base station sends data by encrypting it with the individual keys.

for all $x \in memberList$ **do**
  $B \rightarrow x : E_{K_x}(msg)$
end for

4.3. Hybrid Scheme

- Set Up

  The hybrid scheme uses the concept of *Stable* and *Unstable* users to determine the technique by which the user would receive the multicast data. A member is classified as *Stable* or *Unstable* depending on whether it has been a member of the group for more than a given period of time or not, which in turn depends upon the mobility of the user. This period of time (t_s) serves as parameter for adaptation.

- Join

  Initially all the members are classified as *Unstable* upon entering a cell. In this scenario the base station shares different session keys with each member, making this similar to *DSK*. Refer to algorithm 5.

- Stabilize

  When the soft state timer expires the the member list is scanned for members who have stayed in the group for a period greater than t_s. These members are re-classified as members of the stable subgroup. Whenever such a reclassification occurs the shared session key of

Algorithm 5: The following action is taken when a node enters the service area.

```
beacon = recv()
i = getNodeId(beacon)
if (isPresent(i)) then
  t_i^u = 0
else
  Routine to authenticate user i and exchange
  individual key.
  addToList(i)
  t_i^s = 0
  t_i^u = 0
end if
```

the stable subgroup is changed and the new key is encrypted using the old key and sent to the existing members while the newly stabilized member receives it encrypted with its individual key. Refer to algorithm 6

- Leave

  When a user leaves the group the key management action depends on whether the departing user is a stable user or unstable user. When an unstable user departs its individual key is just discarded. But if a stable user departs the session key of the stable subgroup is changed and it is encrypted with the individual keys of the existing users and unicasted to them. Refer to algorithm 6

- Data Transmission

  The multicast of data in this scheme is achieved in two stages. First the data is encrypted using the group session key of the *stable* subgroup and sent to the group address. In the second step the data is encrypted using the respective individual keys and unicasted to the *unstable* users.

The hybrid scheme is made adaptable by the parameter t_s. This parameter determines whether a member will be reclassified or not. If the time for which the mobile host has been in the service area is greater than t_s, then the mobile host can be reclassified. The parameter t_s

Algorithm 6: The base station executes the following on expiry of soft state timer.

On expiry of soft state timer.
for all $i \in$ memberList **do**
  $t_i^u = t_i^u + t^b$
  $t_i^s = t_i^s + t^b$
end for
if $(hasDeparted())$ **then**
  if $(stableDepart() \| stabilize())$ **then**
    $K_s^{'} = getKey()$
    for all $x \in stableList$ **do**
      $B \rightarrow x : E_{K_x}(K_s^{'})$
    end for
  else
    Discard the key of the departed node.
  end if
  Restart soft state timer.
else
  Restart soft state timer.
end if

where,
t^b is the batch interval after which the base station updates its lists.

Algorithm 7: The base station sends data by in two stages.

$B \rightarrow groupId : E_{K_s}(msg)$
for all $x \in unstableList$ **do**
  $B \rightarrow x : E_{K_x}(msg)$
end for

is determined from the mobility rate of the users and prior history. t_s is not constant for the entire network, but each base station in the network can dynamically configure the value of t_s. We have conducted experiments to determine the optimum value of t_s, the results of which are presented in section 6.3.6. The hybrid scheme requires maintaining a record of position of each member node. The history maintenance starts as soon as the member enters the cell when it is classified as an *Unstable* member. Thus whenever the member enters, a counter is started for that member. If the member remains in the cell for time greater than t_s then it is classified as stable. However, if the member moves out before that time interval elapses then the timer is reset (i.e.) the history is erased. If the value of t_s were higher then the memory required for maintaining the history would increase. However, choosing a small value for t_s may result in nodes that are not totally stable being classified as *Stable*. Thus the value for t_s should be such that the memory requirement is minimized and appropriate reclassification is performed.

CHAPTER 5

ANALYSIS OF THE ALGORITHMS

In this chapter, we present the mathematical analysis of the algorithms presented in the previous chapter. The objective of the analysis is to obtain a comparative view of the performance of the three secure multicast schemes. There exist some aspects which will affect the performance of the schemes when actually implemented. But they will affect all the three schemes similarly. Hence they will not alter the conclusions which we draw from our analysis. The variables used in the analysis are explained in the Table 2.

The probability that n_i nodes out of the total n nodes are inside the service area is obtained by subtracting the probability that they are outside from one. It may be shown as follows

$$p_{ni} = 1 - \left[\binom{n}{n_i} (p_o)^{ni} (1 - p_o)^{n-ni} \right].$$

Table 2. Notation used in Analysis

Variable/Function	Description
T_s	The time for which the protocol is studied.
R	The rate at which data is multicasted.
C_e	Cost of encryption.
C_{ke}	Cost of key establishment.
C_u	Cost of unicasting a packet.
$C_{D,sch}$	Total Cost of multicasting data for scheme *sch*
$C_{K,sch}$	Total Cost of key management for scheme *sch*
C_{sch}	Total Cost for scheme *sch*
p_m	Probability of mobility of a node.

Here we assume that p_o; the probability of a single node being out side the service area, to be directly dependent on the mobility. Hence it is equated to p_m. Hence the above equation reduces to

$$p_{ni} = 1 - \left[\binom{n}{ni} (p_m)^{ni} (1 - p_m)^{n-ni} \right].$$

The total cost consists of two parts namely, the cost of data transmission and the cost ok key management. The costs are calculated as follows.

5.1. Single Session Key

For the SSK scheme the cost of data transmission is equal to cost of broadcasting the data to all the nodes inside the service area. It is given by

$$C_{D,SSK} = T\ R\ (C_e + C_u).$$

The cost of key management includes cost of rekeying the whole group, when a node leaves the group or a new node enters the group. It is given as

$$C_{K,SSK} = p_m\ n_i\ C_{ke}.$$

Hence the total cost is given by

$$C_{SSK} = p_{ni}\ (T\ R\ (C_e + C_u) + p_m\ n_i\ C_{ke}).$$

5.2. Different Session Key

For the DSK scheme the cost of data transmission is equal to the cost of unicasting the data to each and every node inside the service area. It is given by

$$C_{D,DSK} = T\ R\ (C_e + C_u)\ n_i.$$

The cost of key management is due to establishing a key with a new node, when it enters the group. It is given as

$$C_{K,DSK} = p_m \; C_{ke}.$$

Hence the total cost is given by

$$C_{DSK} = p_{ni} \; (T \; R \; (C_e + C_u) \; n_i + p_m \; C_{ke}).$$

5.3. Hybrid Scheme

For the Hybrid scheme the cost data transmission is equal the to sum of multicast to the stable members and unicast to each one of the unstable members. It is given as

$$C_{D,Hybrid} = T \; R \; (C_e + C_u) \; (1 + n_i \; (1 - p_m)).$$

The cost of key management consists of costs incurred in three situations. They are to establish a new key when a new node enters enters the service area, when rekeying the group of stable users when a stable user leaves the service area and, when rekeying the group of stable users when a unstable user is stabilized. It is given as

$$C_{K,Hybrid} = p_m \; C_{ke} + p_m \; p_m \; n_i \; C_{ke} + 2 \; (1 - p_m) \; C_{ke}$$

Hence the total cost incurred for the Hybrid scheme is given by

$$\begin{aligned} C_{Hybrid} = \; & p_{ni} \; (T \; R \; (C_e + C_u) \; (1 \; + \; n_i \; (1 - p_m)) \\ & + (p_m \; C_{ke} + p_m \; p_m \; n_i \; C_{ke} \\ & + 2 \; (1 - p_m) \; C_{ke})) \end{aligned}$$

The results of the above analysis are as shown in the figure 2. It may be observed that at high mobility the hybrid scheme involves less cost. This conclusion is in line with our simulation results which will be presented in chapter 6.

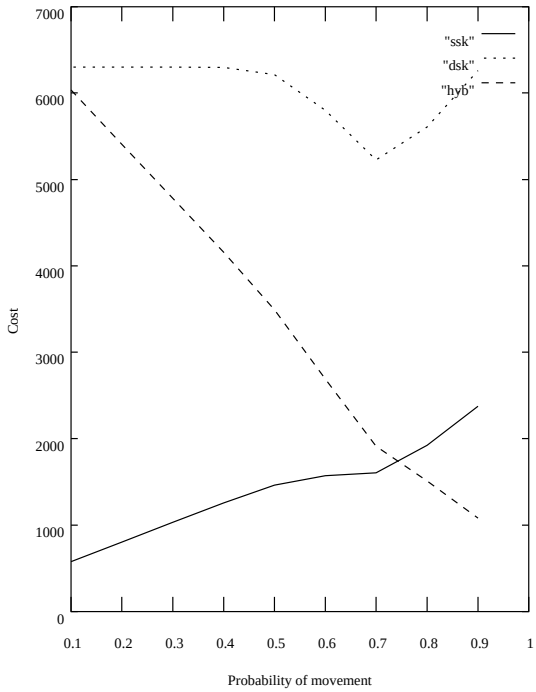

Figure 2. Analytical Comparison of the three schemes

CHAPTER 6

PERFORMANCE EVALUATION AND RESULTS

In this chapter, the simulations performed in order to study the performance of the schemes for secure multicast described in the previous chapters are presented. The Network Simulator-2 is used to simulate the algorithms described earlier. The simulator basics are described briefly. Then the simulation environment is described. This includes properties of the nodes, their mobility patterns and the performance metrics that have been used to evaluate the proposed schemes. Following this, the simulation results are presented. The chapter is concluded by making some inferences from the simulation results.

6.1. Network Simulator

The Network Simulator (NS-2) is a discrete event simulator with support for various layers of the network protocol stack like Medium Access (MAC), Network, and Transport layers. The Simulator code as such consists of two components. One is TCL and the other in C++. The TCL part forms the front end. The node configurations such as kind of routing, medium access protocols to be used, the transmission energy and so on are specified in the TCL part. Other specifications such as initial node placements, events like node movements, data traffic generation are specified in the TCL files. The actual protocols are implemented in the C++ part. The implementation in C++ responds to the events generated by the TCL code.

6.2. Simulation Environment

In this section the simulation environment is described. The schemes have been implemented at the Medium Access(MAC) layer of the protocol stack. There exists in NS-2 an implementation of the IEEE 802.11 specification for the medium access. The key management schemes presented in the earlier chapters are implemented as part of the MAC layer. This is as shown in the NS-2 architecture in figure 3.

In the simulations, data packets are generated at a continuous rate. This data is generated at the MAC layer itself. This is done since our objective is to study the effect of key management in a single hop network and does not involve issues like routing. The base station maintains neighborhood information. The base-station checks its table after a specific period of time (t_b) over which the joins and leaves of members are batched. If it finds that rekeying has to be performed then the data is stopped and the rekeying process is started. The need for rekeying may arise or may not arise depending upon the scheme which is being simulated. The code for key management based on different schemes earlier is done in the MAC layer as shown in figure 3. The data generation and the key management form a sub layer in the MAC layer in our simulations.

In the simulations, a multicast subgroup consisting of 25 nodes is taken into consideration. This subgroup represents a base-station in the multicast group and its service area. Each node has a transmission range of 250 meters and a bandwidth of 2Mbps. These nodes transmit a beacon to the base station periodically (t_{be}) indicating their presence. The base station maintains a soft state about the neighborhood based on these periodic beacons. The nodes keep moving in and out of the service area. The ***scengen*** tool with random way point model available for NS was used to generate random movement of the mobile hosts.

For each of the schemes a simulation is run for a fixed duration of 300s. The energy consumed by the system, for the multicast of 1000 packets is measured. This energy includes both the energy consumed for multicasting the data packets as well as the energy consumed for

Table 3. Parameters used in the simulations

Parameter	Value Used
Batch Interval (t_b)	0.1 secs
Beacon Interval (t_{be})	0.01 secs
Number of Packets	1000
Simulation Time	300 secs

performing the key distribution. Thus the total energy is the sum total of the energy consumed by all the nodes in the system. Such simulations are performed till the required level of confidence is achieved.

The parameters used in the simulations are summarized in table 3.

6.3. Performance Comparison

In this section the actual performance comparisons between the three algorithms presented earlier are presented. The algorithms' performance are compared pairwise. Performance with improvements based on key multicast and batching mentioned in chapter 2 have been compared with performance when they are not incorporated. Finally the performance of the HYBRID scheme while varying the adaptability parameter t_s is presented.

6.3.1. Comparison of DSK and SSK. For low mobility rates the energy consumed for SSK scheme is lower as compared to DSK. This due to the fact that when mobility is low the number of joins and leaves is low. This in turn lowers the number of rekeyings and hence the key management part of the total energy is lower than the data communication energy. Since SSK multicasts data while DSK unicasts it after encrypting it with different keys the data communication energy consumed for DSK is more than that of SSK. But in case of high mobilities the key management cost of SSK dominates over the data communication cost. Hence the total energy consumed increases rapidly in case of SSK. Whereas in case of DSK even at high

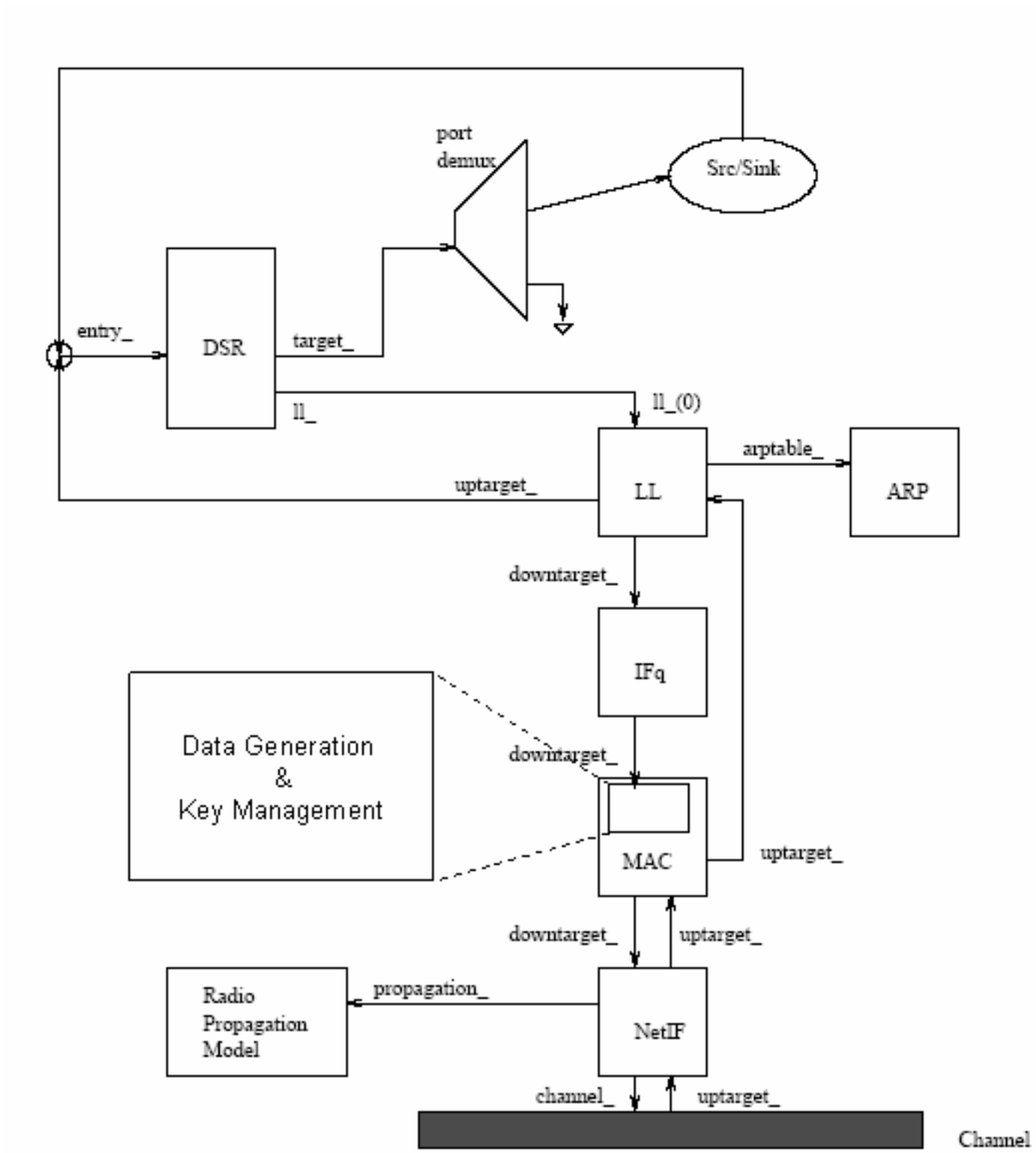

Figure 3. Network Simulator Architecture.

mobilities the data communication energy cost prevails. Hence it performs better than SSK at high mobilities.

6.3.2. Comparison of SSK and the Hybrid Scheme. The hybrid scheme perform better than SSK depending on the mobility rate of the nodes. If the nodes are highly mobile, then frequent change of session keys would be required. This is overcome in the hybrid approach since a node does not share the same session key until it becomes stable. However, if the nodes are pretty static with respect to the base station after joining the multicast, then an overhead is incurred in the hybrid scheme to move those nodes from the *Unstable* group to the *Stable* group.

6.3.3. Comparison of DSK and the Hybrid Scheme. In DSK all the nodes have a different session key even though nodes that are fairly immobile with respect to the base-station could share the same session key. The hybrid scheme moves such nodes into the *Stable* group thereby reducing the communication overhead. This brings in an element of the multicast paradigm. The communication cost required to send the data to all the nodes is reduced for the HYBRID scheme since the data is multicasted for a subset of the mobile nodes.

6.3.4. Performance with Batching. Figure 5 shows the performance of the Hybrid scheme when the join/leave events are batched and when they are not batched. From the figure it may be observed that the scheme performs better when the events are batched at high mobilities. This improvement in performance may be attributed to the fact that the rekeying which are required in a batch interval are merged into one in batched scheme, while this is not the case when batching is not done.

6.3.5. Performance with Multicasting for key distribution. Figures 6 shows the performance of the HYBRID scheme when multicasting is used for key distribution as explained

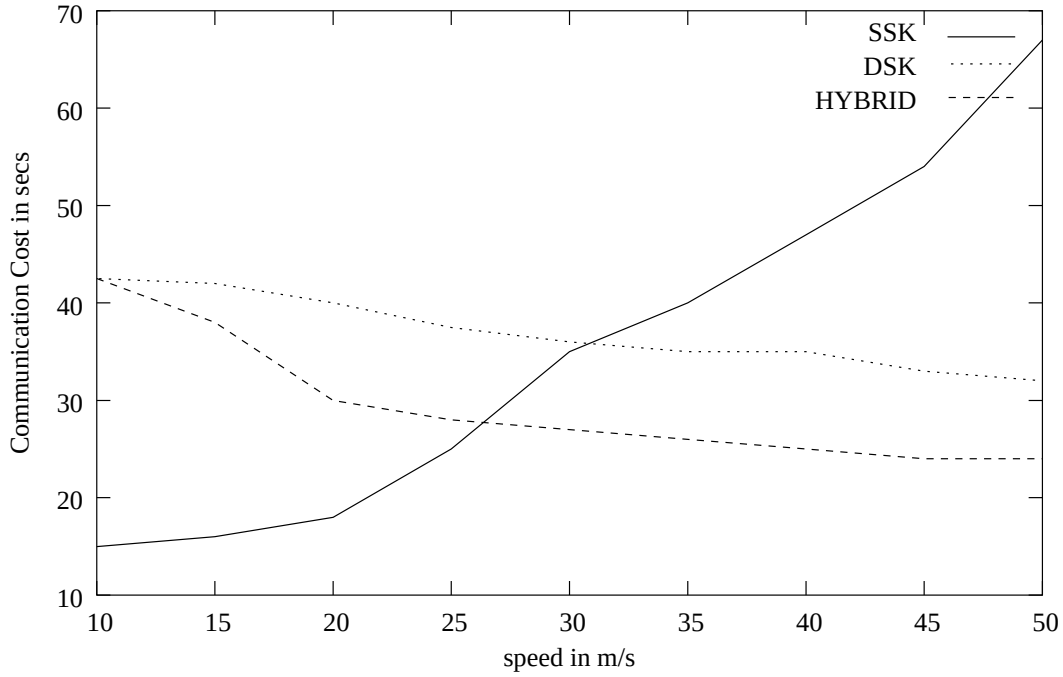

Figure 4. Comparison of the three schemes

in section 2.4 and when it is not used . Performance improves with multicasting due to reduction in number of transmissions by base-station.

6.3.6. Adaptability of Hybrid scheme. Results of experiments performed to determine the optimal value of t_s for Hybrid scheme are shown in figure 7, 8, 9. As mobility increases the communication cost varies significantly and the scheme performs better with higher values of t_s. But this trend reverses after a certain point ($t_s = 8$). This is because at high mobility, the probability that a node moves out after a particular time is high. So it is desirable that we wait for longer time before we classify the mobile host as stable because of the overhead involved in rekeying, if a stable node leaves is high. But if we wait for too long, mobile hosts which are eligible for classification as stable remain as unstable for longer time. Hence data is unicasted them instead of including them in the multicast group. This overhead exceeds the overhead of rekeying. Thus a value of t_s which balances both overheads is to be chosen.

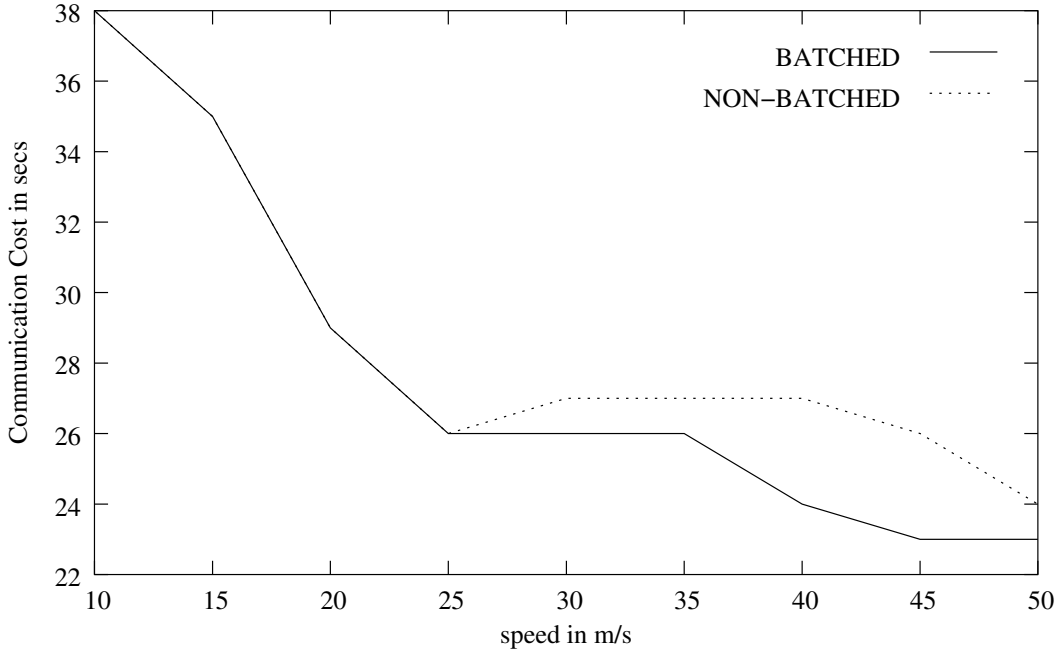

Figure 5. Performance of Hybrid scheme with and without Batching

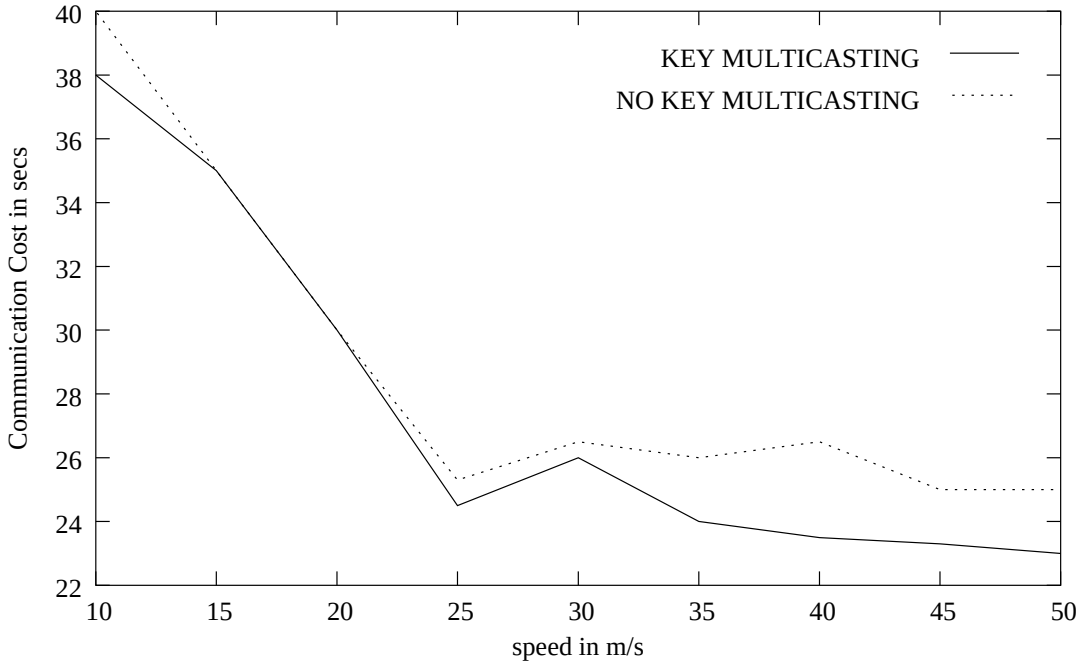

Figure 6. Performance of Hybrid scheme with and without key-multicast

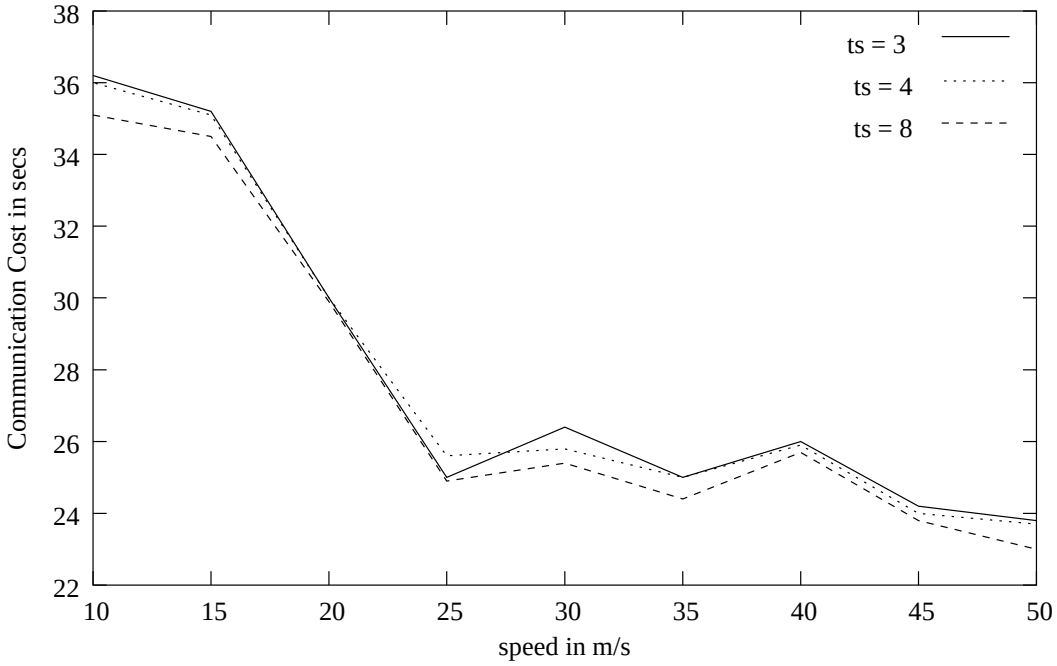

Figure 7. Performance of Hybrid scheme with variation in t_s

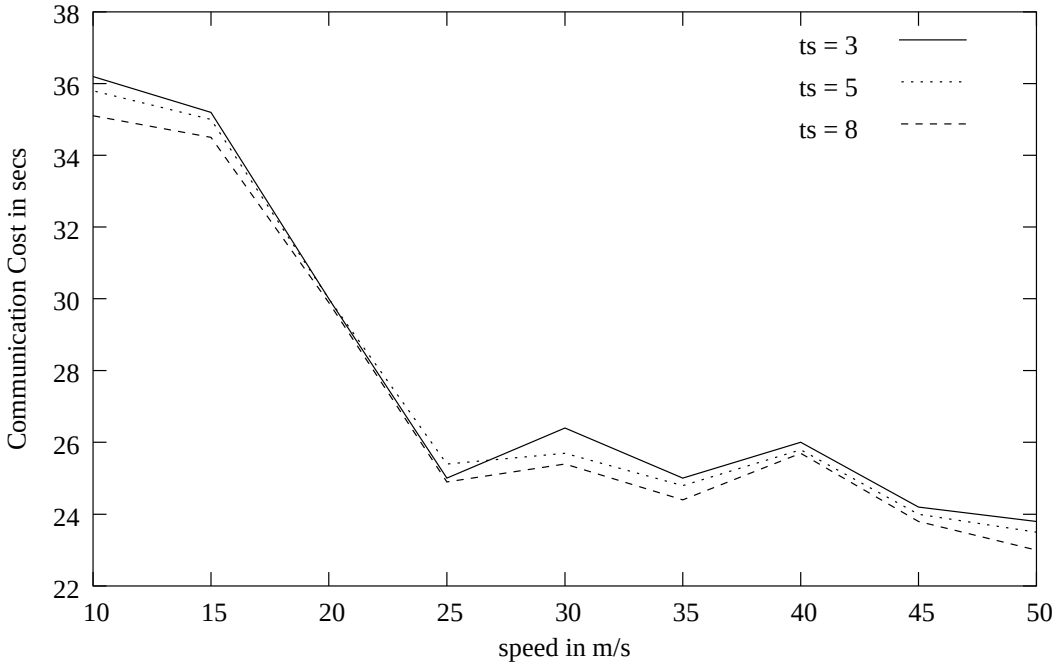

Figure 8. Performance of Hybrid scheme with variation in t_s

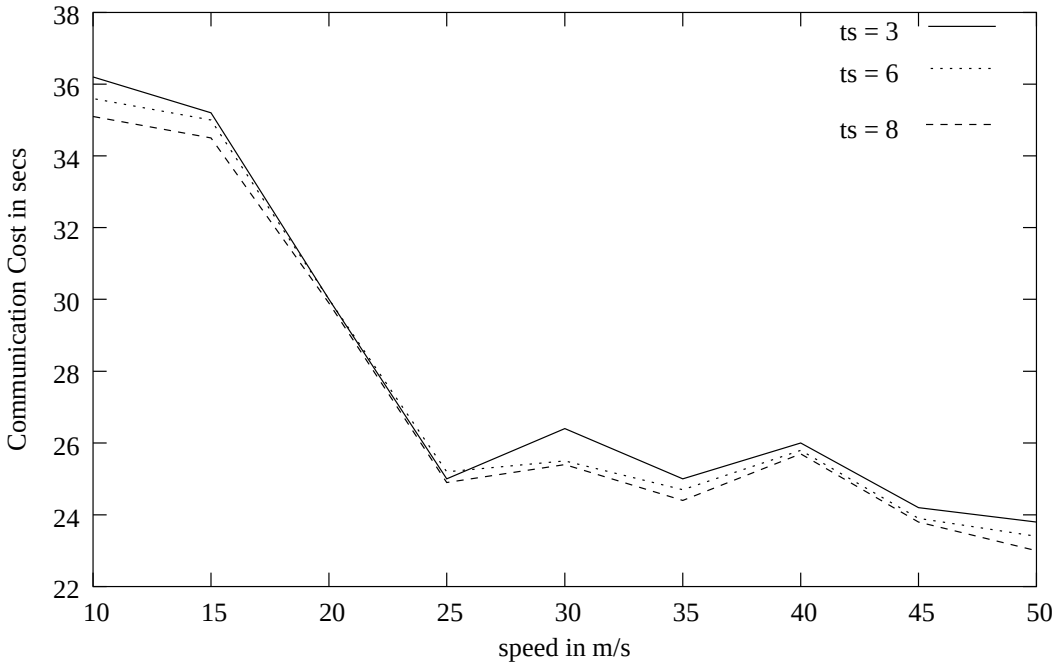

Figure 9. Performance of Hybrid scheme with variation in t_s

CHAPTER 7

CONCLUSIONS AND FUTURE WORK

Group communication models have gained a lot of popularity. They are of special significance in wireless networks like wireless Local Area Networks (LANs). There exist a large number of applications for group oriented services in such scenarios. Many of these applications require that the multicast data be secure. Security includes properties such as confidentiality, integrity, authenticity. In addition to these requirements additional requirements are introduced in group or multicast communications. These are forward message secrecy and backward message secrecy. Achieving these security requirements in wireless networks with mobile users poses an difficult problem since wireless networks have constraints like low energy, low computation and communication capabilities.

In this thesis, the issues related to secure multicasting such as constraints and requirements have been identified. Among them mobility poses a very significant challenge as it causes the group membership to be highly dynamic. In this thesis, three solutions possible solutions are proposed to achieve the security requirements of secure multicast. The three schemes vary based on whether the base station shares the same session key with all the members of multicast group or different session keys with each member, or a combination of the two. The third scheme (Hybrid scheme) is an adaptive scheme where some of the users are classified as stable based on the duration for which they have resided in the group. The threshold duration serves as the parameter for adaptability.

It has been observed that for wireless LANs which are prone to moderate to high dynamic behavior, the Hybrid scheme performs better than the other two schemes due the introduction of multicast paradigm in data transmission and the reduction in the number of key setups. We have also used the concepts of batch processing and multicasting in key management to optimize the cost. Within the Hybrid scheme we are able to adapt to the mobility, thereby reducing the cost further. The optimal value of adaptability factor has been determined.

This chapter is concluded with a note about the possible future work. In this research we used the idea of grouping the multicast group users into two groups based on the mobility of the users. This lead to improved performance. It needs to be examined whether increasing the number of such groups would lead to an improved performance. If so then what would be the ideal number of group and what would be the factors which would determine the number of groups? In this research only mathematical analysis and simulations have been used to examine the performance. The actual implementation will further be useful in analyzing the performance of the schemes presented in this research.

REFERENCES

[1] Vaduvur Bharghavan. Secure wireless LANs. In *ACM Conference on Computer and Communications Security*, pages 10–17, Fairfax, VA., 1994.

[2] D. Bruschi and E. Rosti. Secure multicast in wireless networks of mobile hosts: protocols and issues. *Mobile Networks and Applications (MONET)*, 7, Issue 6:503–511, December 2002.

[3] S. Cherukuri and S.K.S. Gupta. An adaptive protocol for efficient and secure multicasting in IEEE802.11 based wireless LANs. In *IEEE Wireless Communications and Networking Conference, WCNC*, pages 2021–2026, New Orleans, 2003.

[4] IEEE Computer Society LAN MAN Standard Committee. Wireless LAN medium access control MAC and physical layer specifications, IEEE Std 802.11. *The Institute of Electrical and Electronics Engineers*, 1999.

[5] M. Corner and B. Noble. Zero Interaction Authentication. In *Conference on Mobile Computing and Networking (MobiCom)*, September 2002.

[6] L. R. Dondeti, S. Mukherjee, and A. Samal. A dual encryption protocol for scalable secure multicasting. In *Proceedings of IEEE International Symposium on Computers and Communications*, pages 2–8, Red Sea, Egypt, 1999.

[7] A. Eskicioglu. Multimedia security in group communications: Recent progress in wired and wireless networks, 2002.

[8] Kevin Fall and Kannan Varadhan. The ns manual (formerly ns notes and documentation).

[9] J. Kuri and S. K. Kasera. Reliable multicast in multi-access wireless lans. In *Proceedings of Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM*, volume 2, pages 760–767, March 1999.

[10] J. Kuri and S.K. Kasera. Reliable multicast in multi-access wireless lans. *ACM Wireless Networks*, 7, Issue 4:359–369, 2001.

[11] Xiaozhou Steve Li, Yang Richard Yang, Mohamed G. Gouda, and Simon S. Lam. Batch rekeying for secure group communications. In *Proceedings of the tenth international World Wide Web conference on World Wide Web*, pages 525–534, Orlando, FL USA, 2001.

[12] Suvo Mittra. Iolus: a framework for scalable secure multicasting. In *Proceedings of ACM SIGCOMM conference on Applications, technologies, architectures, and protocols for computer communication*, pages 277 –288, Cannes, France, 1997.

[13] Naveen Sastry, Umesh Shankar, and David Wagner. Secure verification of location claims. In *Proceedings of the 2003 ACM workshop on Wireless Security*, pages 1–10, 2003.

[14] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition.* Wiley, New York, 1994.

[15] Marcel Waldvogel, Germano Caronni, Dan Sun, Nathalie Weiler, and Bernhard Plattner. The versakey framework: Versatile group key management. *IEEE Journal on Selected Areas in Communications*, 17(9):1614–1631, September 1999.

[16] Roy Want, Andy Hopper, Veronica Falcão, and Jonathan Gibbons. The Active Badge Location System. Technical Report 92.1, Olivetti Research Ltd. (ORL), 24a Trumpington Street, Cambridge CB2 1QA, 1992.

[17] Chung Kei Wong, Mohamed Gouda, and Simon S. Lam. Secure group communications using key graphs. In *Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication*, pages 68–79, 1998.

[18] Lidong Zhou and Zygmunt J. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, November 1999.