Reliable Communications over Heterogeneous Wireless Networks

by

Hany Samuel

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2010

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

The recent years have seen an enormous advance in wireless communication technology and co-existence of various types of wireless networks, which requires effective inter-networking among the heterogeneous wireless networks in order to support user roaming over the networks while maintaining the connectivity. One of main challenges to achieve the connectivity over heterogeneous wireless networks is potential intermittent connections caused by user roaming. The issue is how to maintain the connection as the user roams and how to ensure service quality in the presence of a long disconnection period.

In this dissertation, we apply the delay tolerant network (DTN) framework to heterogeneous terrestrial wireless networks, and propose a system architecture to achieve the connectivity in the presence of excessive long delays and intermittent paths. We study several possible approaches, discuss the applicability of each of the approaches and propose the super node architecture. To demonstrate the effectiveness of the proposed super node architecture, we give a simulation study that compares the system performance under the super node architecture and under the epidemic based architecture.

Within the proposed architecture that employs the idea of super nodes, we further study how to effectively route a message over access networks. We present a new routing technique for mobile ad-hoc networks (MANETs) based on the DTN system architecture. We introduce the concept of virtual network topology and redefine the dominating-set based routing for the challenged network environment under consideration. In addition, we propose a time based methodology to predict the probability of future contacts between node pairs to construct the virtual network topology. We present a simulation study that demonstrates the effectiveness of the proposed routing approach as compared

with the epidemic routing, and that the time based technique for predicting the future contacts gives better performance compared with that using the number of previous contacts.

We further extend the dominating set routing technique through analyzing the underlying node mobility model. We shed some light on how using node mobility model can improve contact probability estimation. Based on our findings we propose a new algorithm that improves the routing performance by minimizing the selected dominating set size.

Information security challenges in the super node architecture are introduced. We further address two main security challenges: The first is how to prevent unauthorized nodes from using the network resources, and the second is how to achieve end-to-end secure message exchange over the network. Our proposed solutions are based on asymmetric key cryptography techniques. Moreover, we introduce a new idea of separating the problem of source authentication from the problem of message authorization. We propose a new technique that employs the one-way key chain to use symmetric key cryptographic techniques to address the problems under consideration.

Acknowledgements

First and foremost, I would like to express my sincere appreciation to my supervisor, Prof. Weihua Zhuang. I thank her for her continuing guidance and support during my whole Ph.D. research. Without her vision, advices, extensive knowledge, strong analytical skills and commitment to the excellence, this thesis would not have been possible. Her great enthusiasm has been the main supporting power for the completion of this thesis. I have learned so many things from her not only on the technical side but also on the personal side. I would like to thank her for providing the necessary funding for making this research possible. I genuinely thank her for encouraging and inspiring me in each step, her ceaseless encouragement have made this research and our collaboration an exciting experience which I am genuinely proud of.

I would like to express my genuine appreciation to my thesis committee members: Prof. Gordon B. Agnew, Prof. Liang-Liang Xie , Prof. Guangzhe Fan and Prof. Peng-Jun Wan. They have devoted precious time and efforts for my thesis and have helped me to improve it. Their insightful comments and invaluable suggestions are genuinely appreciated.

Also, I would like to thank and express my gratitude to my professors and colleagues at the BBCR group. I would like to devote a special appreciation to Prof. Xuemin (Sherman) Shen for his ceaseless help and support. I have learned a lot from his deep research experience and invaluable advices.

Finally, I would like to dedicate this thesis to my beloved wife, Noha, and my daughters, Carla and Tia. I hope I can make it up to them for all the time they sacrificed to help me to be devoted to my study.

To Noha, my beloved wife, and to my adorable daughters, Carla and Tia

Table of Contents

List of Figures

List of Tables

List of Notations

S_A	The super node of node A
$G(V, E)$	A graph G with set of vertices V and set of links E
$NG(i)$	Set of neighbour vertices of node i
DS	Dominating set
π_i	Limiting probability of a Markov chain for state i
τ_{ij}	The inter-meeting time between node i and node j
τ_i	The inter-meeting time between node i and DS
θ_t	The threshold value for selecting the dominating set
ID_A	The public identifier of entity A
$\|$	Message concatenation operation
PK_A	The public key of node A
SK_A	The private key of node A
$Enc_K(\cdot)$	Symmetric key encryption function with key K
$Dec_K(\cdot)$	Symmetric key decryption function with key K
K_i	Symmetric key with index i in one-way key chain
$E_X(\cdot)$	Asymmetric key encryption function with key X
$D_X(\cdot)$	Asymmetric key decryption function with key X
$H(\cdot)$	One-way hash function such as SHA-1

$H^i(\cdot)$	Applying hash function H for i times
$HMAC_K(\cdot)$	A keyed-hash message authentication code using key K
KG_n	A key group of length n
$G(\cdot)$	Private key generating function for IBC technique
PP	The public parameter for Private Key Generator (PKG)
CA	Certificate Authority
$Cert_{CA_n}(B)$	A certificate issued for node B for time interval n
$K_{CA,B}$	A shared secret key between node B and the certificate authority

List of Abbreviations

DTN	Delay Tolerant Network
MANET	Mobile Ad-hoc Network
ITS	Intelligent Transportation System
WLAN	Wireless Local Area Network
TCP	Transport Control Protocol
UDP	User Datagram Protocol
TTL	Time To Live
TC	Traditional Cryptography
IBC	Identity Based Cryptography
AAA	Authentication Authorization Accounting
PKI	Public Key Infrastructure
PKG	Private Key Generator
iid	Independent and Identically Distributed
AES	Advanced Encryption Standard
SHA	Secure Hash Algorithm
TESLA	Timed Efficient Stream Loss-tolerant Authentication protocol
ECDSA	Elliptic Curve Digital Signature Algorithm
GF	Galois field

ECC	Elliptic Curve Cryptography
CRL	Certificate Revocation List
ID	Identifier
MSG	Message
HAB	Huge anonymous keys based protocol
RSU	Roadside unit
VHR	Virtual Home Region
LAN	Local Area Network
VANET	Vehicular Ad-Hoc Network
ECQV	Elliptic Curve Qu-Vanstone
NSA	National Security Agency
NIST	National Institute of Standards and Technology
DES	The Data Encryption Standard
3TDEA	Triple DEA block cipher that is formed from the DES cipher by using it three times with 3 keys
2TDEA	Triple DEA block cipher that is formed from the DES cipher by using it three times with 2 keys
IFC	Integer Factorization Cryptography
ECMQV	Elliptic Curve Menezes Qu Vanstone
ECDH	Elliptic Curve Diffie-Hellman
LR-WPANs	Low-Rate Wireless Personal Area Networks

Chapter 1

Introduction

Over the recent years, wireless technology has been gaining momentum with a wide spread of wireless networks. Various types of wireless networks have been deployed and widely used, such as 3rd-generation cellular networks, wireless local area networks (WLANs), sensor networks, and mesh networks. Each type of network is optimized for a specific networking environment, and it is impossible to have only one type of wireless network that suits all the environments. The global information transport platform via internetworking has become an incontrovertible fact, regardless of the differences among these networks either in structure or in protocols used over them. This leads to the existence of heterogeneous wireless networking.

Achieving continuous connection for roaming users over heterogeneous wireless networks is a difficult (if not impossible) task due to many challenges. One main challenge is how to overcome intermittent connections to users. Intermittent connections cause problems not only for users roaming over different networks, but also for users staying connected to the same network. We propose [1–7] a system architecture that overcomes these problems by adopting the

recently proposed delay tolerant network (DTN) architecture.

1.1 Intermittent Connections

One main problem facing wireless networks is the gaps in network coverage, which causes frequent disconnections and reconnections. These intermittent connections introduce a serious challenge to preserve user sessions especially for a long disconnection period.

No general solution for the problem of intermittent connections has been proposed. Most of the work done to overcome the problem depends mainly on modifying the application layer protocols or using a middleware layer to tolerate these intermittent connections for specific applications. For example, to make transactions resilient to intermittent connections, a middleware called MobileTrans is employed in [8] to force the transactions to adapt to the mobile environment. In [9], the transaction throughput is increased by increasing the execution time and relaxing the consistency properties of transactions. Making a file system resilient to intermittent connections is addressed by many research efforts such as the PRAYER file system (PFS) [10] that creates a mobility-aware file system. Also, the work in [11] addresses how to enhance the web searching for intermittent connected users. This is done by using an Internet proxy to prefetch pages in order to increase the number of relevant results returned to mobile users during their limited connectivity times.

Another reason of having intermittent connections is user roaming over different networks, such as cellular networks, wireless local area networks, and mobile ad-hoc networks (MANETs). The problem here is more complicated because, upon reconnection at a different network, the user identity (*e.g.*, IP address) will be changed. Achieving continuous connectivity in this case implies

a migration of the user's connection information to the new jurisdiction (*i.e.*, network). The problem gets even more complicated when the networks have different owners. Many solutions are proposed [12] for addressing the problem of achieving seamless mobility for roaming users. These solutions focus on different layers of the protocol stack. Some solutions are based on the network layer such as *IDMB* [13], *Mobile IP* [14], *Cellular IP* [15], and *HAWAII* [16], while some others are based on the link layer [17–19]. There are also solutions based on cross-layer design between the link layer and the network layer [20–23].

A problem with all these techniques is mainly due to the potential long disconnection period. When a user is disconnected for an extended period, all these techniques will time out and terminate all the user connections. This makes the techniques unsuitable when no restrictions are assumed on the disconnection time. This research addresses the problem by proposing a new technique to tolerate intermittent connections and long disconnection periods.

1.2 Research Objectives

This research mainly studies the problem of maintaining the connectivity to a user while the user roams over interconnected heterogeneous wireless networks. We address the problem of intermittent connections by applying the DTN framework.

Our main objective is to develop network control algorithms and protocols for providing a virtually continuous connection to roaming users over interconnected heterogeneous wireless networks. Any user can leave the current network and disconnect for a period of time. Then the user can reconnect to the same network or another wireless network while continuing with the old session as if no disconnection occurred.

To the best of our knowledge, no previous research has addressed this problem. Some previous studies have investigated the problem of providing a seamless roaming. The previous techniques cannot maintain the user connection in the presence of potential long disconnections. Dealing with the interconnected heterogeneous wireless networks as a challenged network is the key issue in our research based on the DTN architecture for message exchanges. This new formulation of the problem poses new constraints and new challenges such as in routing and in supporting information security. Many research works have addressed DTN routing and security issues, but they either cannot be directly applied to our problem domain or they are totally inapplicable. We will discuss these technique and compare them with our proposed techniques.

Our research goals include:

- Introducing a networking architecture for message exchanges. This architecture should ensure virtually continuous connectivity for roaming users;
- Providing a routing strategy that guarantees successful message delivery with efficient network resource utilization;
- Ensuring system security in terms of end-to-end secure message exchanges and authorized access to system resources.

1.3 Outline of the Thesis

This thesis is organized as follows. Chapter 2 reviews some important background on challenged networks and the DTN architecture, and presents a brief review of important research issues in DTN routing. Chapter 3 describes the system model and proposes the new networking architecture based on super nodes.

Also, it presents a comparison between the proposed architecture and other possible approaches supported by a simulation study. Chapter 4 discusses routing over the proposed networking architecture and introduces a novel technique for routing over MANETs. Chapter 5 extends the proposed routing technique based on node mobility analysis and discusses how the routing performance can be improved. Chapter 6 introduces two main security challenges within the proposed system architecture. It reviews some research efforts that adapt the traditional asymmetric techniques to achieve security over DTN and then introduces two novel techniques based on a one-way key chain to provide secure message delivery and to prevent unauthorized node from using the network. Chapter 7 provides conclusions of this research and further research directions.

Chapter 2

Literature Review and Background

The DTN architecture [24] is recently introduced to facilitate communications in and internetworking for challenged networks.

2.1 Challenged Networks

Challenged networks [25] are networks that satisfy one or both of the following characteristics:

- The communications path between a data source and its destination may never exist;
- The time to send a message from a source to the destination is excessive, *e.g.*, due to limited bandwidth, error probability, or path instability.

Of course, regular networks may exhibit these properties as well, but it is assumed that these properties are rarely encountered and can be neglected for

protocol design in regular networks. Regular networks always depend on the existence of an end-to-end path to achieve successful communications. As a result, the protocols developed for regular networks fail to function when used for communications over challenged networks. Challenged networks need new communication protocols that suit the hostile networking environment.

To better explain the nature of challenged networks, we discuss some network examples in the following.

- *Medium challenged networks*: This category contains many network types such as near-earth satellite communications, long distance optical [26] and radio communications (as in deep space communications [27, 28] and underwater communications [29–31]). Main characteristics of these networks are a very long delay encountered, frequent disconnections, or unavailability of the communications link. For example, the movement of a satellite over its orbit causes the connection to be available only at specific times. Some of the disconnections in such networks can be predicted or even scheduled, which can improve message routing.

- *Sparse mobile ad-hoc networks*: The mobile ad-hoc networks are networks with no infrastructure or centralized administration. In spite of the nature of mobile ad-hoc networks, successful communications have been achieved over such type of networks by cooperation among the nodes to maintain multi-hop network connectivity [32–41]. Many techniques have been proposed and deployed for path discovery and packet routing over mobile ad-hoc networks such as AODV [32], DSR [35] and DSDV [38]. All of these routing techniques are proposed under the assumption that there is an end-to-end path between the source and the destination. If the path does not exist, the techniques will announce failure. Sparse mobile ad-hoc

networks [41–45] are characterized by frequent network partitioning that may last for an extended period; so maintaining the multi-hop connectivity becomes infeasible.

- *Sensor networks*: These networks [46] are mainly characterized by limited end-node capabilities in terms of memory, processing, and power [47]. A sensor network in general consists of a number of sensors that collect data and report these data back to an entity usually called the sink. The size of the network can be in a range of thousands or even millions of nodes. The field of sensor networks has seen extensive research efforts [48–51]. Due to node limited power and sparse nature of the network, an end-to-end physical path is difficult to be established, so data communications can be done through different techniques such as using data mules [52]. One of the main applications of this type of networks is wildlife tracking [36].

- *Vehicular networks*: Vehicular networks [53–55] are expected to be a main component of intelligent transportation systems (ITS). They allow vehicles to communicate with each other as well as with roadside base stations. The main goal of the vehicular networks is to enhance road safety and improve transportation efficiency. Advances in vehicular networks will lead to potential use of vehicles as a data carrier to provide a communications facility between communicating parties that a vehicle encounters during its travel [44, 56, 57]. Due to frequent partitioning of the network, a source node may be unable to establish an end-to-end physical path with the destination node.

2.1.1 Store and Forward Mechanism

When the existence of an end-to-end path is unlikely, one way for message delivery over challenged networks is through asynchronous message forwarding, also known as the store and forward mechanism.

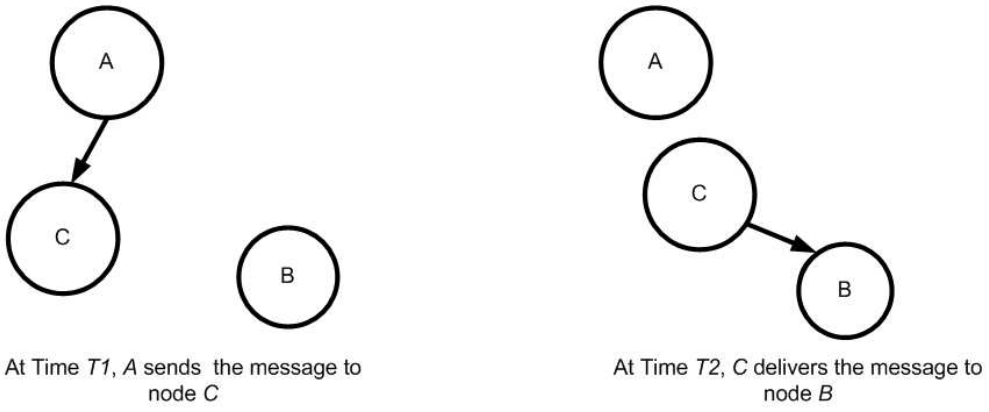

Figure 2.1: Illustration of the store and forward message delivery mechanism.

Consider a simple example as shown in Figure 2.1, a node, A, wants to send a message to a node, B. However, there is no path (either direct or indirect) between nodes A and B. Node C is a mobile node that can communicate with A at time T_1 and communicate with B at time T_2, where $T_2 > T_1$. As node C moves from node A to node B, node A can send the message to node C at time T_1. Node C stores the message and then forwards it to node B at time T_2. Unlike regular networks, the path $A \rightarrow C \rightarrow B$ is *a virtual path* that never fully exists at any time instance. The key step of the communication process is that, node C stores the message and forwards it to the destination or to another intermediate node at a right time.

Challenged networks face mainly two kinds of the challenges: 1) the non-

existence of a path between the communicating parties, and 2) the long communications delay. Indeed, the first challenge can be viewed as a special case of the second challenge.

The previous discussion addresses a simple scenario consisting of only one intermediate node. Routing over challenged networks is to find an intermediate node, or more generally a sequence of intermediate nodes for message forwarding from its source to its destination. This problem is similar to the routing problem in regular networks. However, regular network routing techniques search for a physical end-to-end path, but not a virtual path.

2.1.2 Delay Tolerant Network Architecture

There exist various types of challenged networks, each with its own protocols that limit the possibility of internetworking among different types of networks without the need of a highly specialized proxy. The delay tolerant network architecture [25, 28] is introduced for communications over challenged networks and to help the interoperability among challenged networks. It also facilitates internetworking among challenged networks and regular networks.

The need for a new network protocol architecture is due to the unsuitability of the existing communications protocols for communication over challenged networks. Both network layer and transport layer protocols for regular networks fail to adapt due to long delays and/or the absence of an end-to-end physical path. For example, the Internet routing protocols depend on receiving management messages on regular intervals to discover and keep the paths. With no existence of a physical path and with a long message delay, these protocols will not function properly. Routing protocols for mobile ad-hoc networks do not do better over these networks for the same reason. Both proactive protocols and

reactive protocols assume the existence of an end-to-end physical path. As a result, they fail to adapt to the intermittent nature of the paths in the system.

Even if a physical end-to-end path is discovered by the network layer, conventional transport layer protocols may still fail to work over challenged networks. Connection oriented transport protocols will either fail to establish a connection or falsely detect a disconnection due to long delays encountered. For example, the Transport Control Protocol (*TCP*) will fail because it will time out. This can happen at any phase of the protocol operation. It may happen at the connection setup phase due to the required negotiations. Even if a connection is established, the increasing round-trip latency will demolish the throughput of the TCP over such networks. It will cause the protocol to either falsely detect lost data and start a retransmission or falsely detect a congestion and reduce its transmission rate. The TCP must deliver the data in order, which implies that any lost data will need retransmission. The lost data will also prevent the delivery of all subsequent transmitted data on the same connection, until it is being successfully delivered. This is impractical for a DTN because it limits the data that can be successfully transferred over the existing path. Considering the short life time of a path, it is clear that connection oriented protocols should not be used.

Connectionless transport protocols such as the User Datagram Protocol (*UDP*) are more suitable for communication over challenged networks. They do not require a connection setup and they do not perform any kind of handshaking to ensure message delivery and its order. However, using them will move these functions to a higher layer (*e.g.*, the application layer), which does not solve the problem. This makes the connectionless transport protocols (indirectly) unsuitable for a DTN as well.

One solution for the problem under consideration is to change the existing

protocols to tolerate the potential delay over challenged networks. This solution is impractical, especially if we consider internetworking among challenged networks or between them and regular networks. Another solution is introduced in [28] that uses a middleware layer. The idea is first introduced to create connectivity with nodes located deeply in space (*e.g.*, spacecraft). This implies to connect separate network environments characterized by significantly different sets of physical and operational constraints. The proposed architecture is based on the Internet-independent middleware so that it can use a protocol stack that best suits each environment. The work in [25] generalizes the DTN architecture for all challenged networks. The new layer is called the *bundle layer*, which is added between the application and transport layers in the protocol stack as shown in Figure 2.2. This new layer serves to bridge between different stacks at the boundaries between different networking environments in a standard manner.

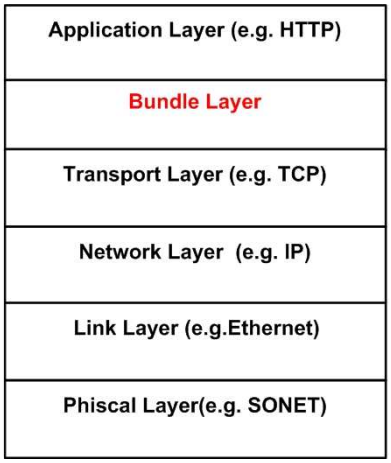

Figure 2.2: The new bundle layer in the protocol stack.

Due to long transmission latency and intermittent paths, the data transmitted should be self-contained. There must be no reliance on any kind of hand-

shaking (*i.e.*, negotiations) or connection setup. The units of data are termed *bundles* (which are similar to email messages). The main function of the bundle layer is to handle sending and receiving of bundles across the network using the underlying protocol stack. It also should hide the nature of the communication environments from the upper layers (mainly the application layer).

2.2 Routing Over DTN

Unlike regular network routing techniques, DTN routing techniques search for a virtual path. In general, the goals for routing techniques in a DTN can be summarized as:

1. *Message delivery:* To ensure successful message delivery is the main goal for DTN routing techniques.

2. *Resources utilization:* There is always a trade-off between efficient resource utilization and improving message delivery rate. Routing algorithms try to achieve the best message delivery rate with efficient resource utilization. The resources include node buffer space, transmission power and bandwidth.

3. *Latency minimization:* Although transmissions over a DTN are expected to have long delays, routing techniques try to minimize the long delays as much as possible.

Successful message delivery in a DTN depends on contacts between a message holder and the message destination. The *contact* can be defined as an opportunity of transmitting and receiving data between two nodes when they fall in each other transmission range for a specific duration. Routing techniques

in a DTN can be classified based on the type of contacts in the network. Contacts in a DTN belong to one of the following categories:

- *Opportunistic:* There is no information available about contact time or place.
- *Scheduled:* It is exactly known in advance when, where and for how long a contact will take place.
- *Predicted:* A prediction of a contact is made based on previous observations such as the last time of meeting or the frequency of meetings among nodes.

There have been many research efforts in DTN routing, some of them are discussed in the following.

2.2.1 Opportunistic Routing

Epidemic routing [58–61] is considered the main technique for opportunistic routing. In epidemic routing, a message source forwards the message to all nodes it encounters. These nodes are called *carriers*. When any two carriers meet, they exchange their carried messages. Message delivery is accomplished when the message destination contacts any message carrier. The main assumption for this technique to succeed is that the node mobility allows any two nodes to move randomly into the communications range of one another. Figure 2.3 shows a partitioned mobile ad-hoc network that contains two disconnected sets of mobile nodes. When node, A, wants to send a message, m, to node, B, it forwards the message to all the nodes it encounters (*i.e.*, node C, and node D). These nodes will become carriers for the message. Each carrier sends the message to all the other nodes it encounters. Each node keeps a vector of all messages it

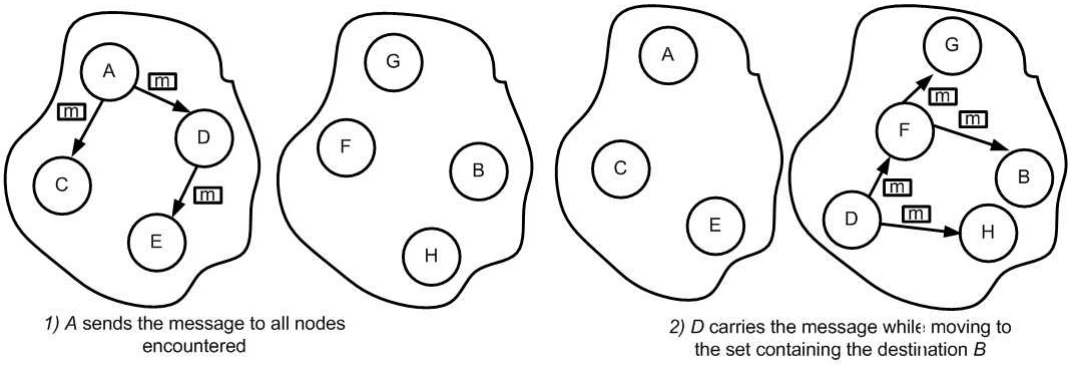

Figure 2.3: Epidemic routing.

contains. When a contact occurs between two nodes, they first exchange their vectors and then they exchange only the messages that are missing. Node C will not send m to node D because node A already sent it to node D. Due to the network partitioning, the message will not be delivered until a carrier comes into contact with a member of the other set that contains the destination node. Node D contacts node F and node H during its mobility outside its set border. When the message reaches one of the set members, it starts to propagate to all the set members until it is delivered to the destination (*i.e.*, node B).

In the previous scenario, there is no need to send the message to nodes C, E, G, H. It would be much more efficient if node A sends the message to node D only, and node D forwards the message to node F. The unnecessary forwarding of the message consumes resources. This deficiency cannot be overcome under the assumption that no information about the system is available.

Epidemic routing tries to create multiple copies of the message over a set of nodes to improve the message delivery rate and delay. In the scenario of Figure 2.3, assuming that node C will meet one of the nodes in the other set nodes, such as node F, node C can send the message to node F, which will

deliver the message to node B. Node C mobility creates an alternative path for the message delivery, but with a longer delay. As a result, epidemic routing guarantees that the message will be delivered with a minimal delay. Due to the message forwarding to all the nodes in contact, the destination is guaranteed to be reached (if it can be reached). Assuming unlimited resources, epidemic routing guarantees the best message delivery rate in addition to the minimum latency. Unfortunately, there are some limitations imposed on the protocol in practice, which limit its ability to achieve the minimum latency and the highest message delivery rate:

- *Buffer space:* Due to limited node buffer space, a node has the right to refuse receiving a message or even to drop some of the received messages to prevent the buffer overflow. One of the proposals [60] suggests that each carrier accepts the message with some probability to overcome the buffer space limitation.

- *Hub count:* It is similar to the TTL field in IP packets. Each message is allowed to be propagated for a limited number of hubs to prevent network flooding. This negatively affects the delivery rate and the delivery latency.

Even when a message is delivered to its destination, other nodes may continue to forward the message. The protocol suggests acknowledging the reception of the message. However, this acknowledgment is intended for the original message sender to confirm message delivery, but not to the carrier nodes to stop forwarding the message. As a result, the hub count field is proposed to solve this problem. Unfortunately, the hub count cannot solve this problem completely, even at the cost of reducing the message delivery probability.

2.2.2 Scheduled Routing Techniques

Routing in interplanetary networks [62] falls under the scheduled routing category. Many techniques and applications have been proposed for a DTN based on scheduled routing. One of these techniques [63] considers the network as a *directed multi-graph* that may have more than one edge (*i.e.*, link) between nodes. This graph is time-varying, but its variations are *known in advance*. In [64], the network is represented as a graph, and the breadth first search is used to find a route between message source and the destination. Based on known future events, the graph is periodically updated; new search is conducted if the processed events update the graph (*i.e.*, adding or deleting edges).

Scheduled routing techniques can use information (other than contact information) such as node available buffer space and communications load. This implies the exchange of a lot of meta information through the network on a regular basis, which is impractical for a DTN. Although it is difficult to achieve in real complicated systems, a trade-off solution can be found based on the actual system constraints. All schedule based routing techniques are not suitable for our problem domain where the movements of users cannot be controlled or scheduled. The main assumption for our problem is the user freedom in roaming.

2.2.3 Predicted Routing

In predicted routing, a message is forwarded to a node based on the probability that this node is able to deliver the message. The probability is calculated based on some criteria such as the number of previous contacts. The number of nodes to forward the message to should be restricted by some factors such as the radio spectrum bandwidth, the node transmission power, and buffer space.

PROPHET [65] uses the idea that a node is most probably to meet with nodes recently encountered. It defines a probabilistic metric called *delivery predictability*, which is the probability that the node will be able to deliver a message to the destination. Each intermediate node calculates the delivery predictability for each known destination, records a vector of all its delivery predictability information. When two nodes meet, they exchange their vectors. Based on the exchanged vectors, they start exchanging messages. After the meeting, each node increases the delivery predictability value of the other node in its vector. Similarly, each node periodically decreases the delivery predictability of nodes not encountered. PROPHET argues that the delivery predictability is transitive. If node A frequently encounters node B, and node B frequently encounters C, then node C is a good node to forward messages destined to node A.

A more general technique that uses a utility function is introduced in [66]. This utility function represents the usefulness of a specific host as a message next hop. This utility function is an indication that this host may meet the destination to deliver the message. The utility function covers five components, each representing a factor in selecting the next host:

- *Most recently noticed:* This is similar to the principle used in PROPHET [65].
- *Most frequently noticed:* This factor examines how frequently the host encountered the destination. It assumes that the host that encountered the destination most frequently is more likely to encounter it next.
- *Future plans:* This factor is similar to the scheduled routing case.
- *Power:* This item is very important for networks with limited end-node

power. The node that is expected to remain alive longer is assigned a larger utility value.

- *Rediscovery interval:* This factor represents how frequently the node tries to discover appropriate hops for carried messages.

The utility function is a weighted sum of all the factors. The weight of each factor depends on how important the factor is regarded.

The idea of routing using a node mobility profile is introduced in [67]. It is assumed that each node has a specific number of locations (*i.e.*, hubs) that it usually visits. It is argued that even if this hub list may vary, the variation will be marginal. *SOLAR-HUB* protocol is a routing protocol based on mobility profile idea. This protocol suggests that a message be routed to one or more locations visited by the receiver when either the sender or an intermediate node visits these hubs. The contact probability between two users is computed based on all user's hub-visited probabilities. It is assumed that each node knows its next hub, so that a node forwards a message to a number of its neighbors which have higher probabilities to visit a hub visited by the destination. Each node is assumed to know every other node mobility, and can compute the contact probabilities with every other node. The information is represented in a weighted graph. Each node applies a variation of the Dijkstra's algorithm to find a list of shortest paths to every other destination. Then it maintains the next hop for each of these paths, but at the time of forwarding, it forwards a message to only the best k paths (where k is determined by the protocol).

A generalization that abstracts the idea of the mobility pattern is introduced in [68]. A message is forwarded to the node that has a mobility pattern similar to that of the destination. Each node calculates its pattern space based on the virtual contact space, where each possible contact is an axis. The distance to

an axis measures the probability of contact. Nodes that have different sets of contacts or same set of contacts with different frequencies are far when calculating the distance between their mobility patterns. This distance is an indication of the possibility of a contact among nodes.

Predication based routing techniques are more suitable for the problem under consideration. There are various previous and concurrent techniques, such as [69–76], proposed to suit different system constraints. In Chapter 4, we will discuss in details how to adopt the concept of predicted routing to our problem domain and proposing a novel routing technique.

2.3 Summary

This chapter provides a brief background of challenged networks. It gives a summary of challenged networks in different categories. After the store-and-forward technique for message delivery over challenged networks is presented, the DTN architecture is introduced. The chapter surveys the different routing techniques for a DTN, and discusses how these techniques are related to the problem under consideration.

Chapter 3

The System Model With Super Nodes

Our focus in this research is how to provide virtually continuous connectivity for roaming users over heterogeneous wireless networks. Considering the interconnected heterogeneous wireless networks as a *challenged network*, we apply the DTN architecture to terrestrial wireless communications, in order to tolerate the potential long delays caused by user roaming. Before discussing the possible solutions, we describe the system model under consideration and make necessary assumptions in the following.

3.1 The System Model

We consider a global information transport platform, which consists of the Internet and a number of heterogeneous wireless networks. The wireless networks include mobile ad-hoc networks, vehicular networks, satellite networks, cellular networks, wireless LANs, and any other networks that allow wireless connectiv-

ity to their users. The size of these individual networks is allowed to be large that the interconnected heterogeneous wireless networks can support a large number of users. We assume that the wireless networks are interconnected over the Internet backbone [77], as shown in Figure 3.1. Each wireless network is

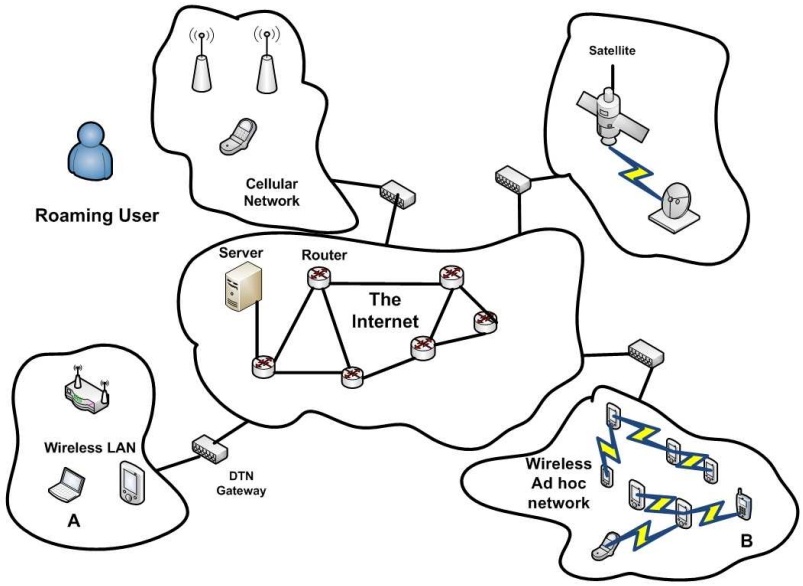

Figure 3.1: Heterogeneous wireless networks connected over Internet backbone.

connected to the Internet through a DTN gateway [25]. The communication between the gateways is reliable over the Internet backbone. Here, we focus on data communications for delay insensitive applications.

Each mobile node (*i.e.*, user) is able to connect to the platform through a subset of the wireless access networks that we call *access networks*. A node may be connected for a period through one access network, disappear for an extended period, and then reappear from the same access network or from a different access network. The node connection over the access networks can be intermittent with frequent disconnections. Any node may move and connect

through any encountered available type of the networks. The problem is how to maintain the connection for that node during its roaming. To better understand the problem, consider the following simple scenario: A user is surfing the web while walking from her car and moving to her office in a building. While she is outside the building, she is connected through a cellular network. As she enters the building, she is disconnected from the cellular network and remains disconnected for a few minutes when she is in an elevator. When she reaches her office, she is able to connect but through a WLAN this time. How to deliver messages to the user in the presence of the disconnection? When the disconnection continues for an extended period, how to store the messages to be delivered to the user upon reconnection at any time and through any network? These are the main questions of interest in this research.

To deal with a potentially long delay encountered in the presence of frequent disconnections, the only effective way for successful message delivery is to use the asynchronous message forwarding mechanism, known as *store and forward* mechanism discussed in Section 2.1.1. It is achieved by relaying messages based on the introduced layer (Bundle layer) in the DTN framework.

We assume that each user has a unique ID that is independent of the current access network. This ID is different from the user ID through the network (*e.g.*, IP address). This ID can be assigned through the DTN layer (*i.e.*, the bundle layer), so it does not interfere with the other layers. The only restriction on the user ID is its uniqueness, so it is assigned by the network management system (*e.g.*, using the cellular phone number).

Supporting user roaming over heterogeneous wireless networks imposes some requirements on the physical layer and the medium access control (MAC) layer. These requirements involve how to design a transceiver for connecting to different networks. For the case of overlapping network coverage (*e.g.*, a cellular

network and a WLAN), the decision on which network to connect to involves many factors such as the signal strength and the connection cost. These questions are out of the scope of our research. In this research, we assume that the underlying layers in the protocol stack are reliable in terms of detecting, connecting, and sending a message in the network.

3.2 Super Node Architecture for Routing

The proposed solution [7] is mainly based on using the DTN architecture so that the applications can use functions provided by the bundle layer to communicate with roaming users. The self-contained nature of the messages (*i.e.*, bundles) solves the problem of establishing and maintaining a connection with the user to achieve reliable communications. The problem now can be reduced to three issues.

1. *Locating a node:* As the node roams, its location is not fixed. The node can be connected via any wireless network at any time. Thus, the first challenge is to locate the destination node in order to communicate with it.

2. *Storing messages:* With the expected disconnectivity and/or the possibility of no existing end-to-end path, a message to be sent to an unreachable (*e.g.*, disconnected) node needs to be stored at some other node(s) and to be forwarded to the destination whenever possible.

3. *Delivering stored messages:* Upon destination node reconnection, the stored messages should be delivered to the node.

Any proposed scheme should address the three aspects of the problem. The objectives in finding a suitable scheme should include the following.

- *Reliable message delivery:* Achieving successful message delivery is the main goal. Successful message delivery should not depend on the availability of the destination node at the time of message generation.

- *Efficient resources utilization:* There is always a trade-off between utilizing resources efficiently and improving the message delivery probability. In general, routing should achieve an optimum message delivery rate with efficient resource utilization. The resources include node buffer space, node power, and the system radio bandwidth.

In the following, we first discuss two possible solutions, and then propose our main scheme based on a concept of super nodes.

3.2.1 Epidemic Routing Based Scheme

The first possible solution makes use of the *epidemic routing* idea [58] that is discussed in Section 2.2.1. This solution assumes no knowledge of user location or availability. It is a distributed routing approach that delivers messages using a flood-like technique. To better understand the solution, consider a simple scenario. As shown in Figure 3.1, if a node, A, wishes to send a message to another node, B, according to the epidemic routing, node A should forward the message to all the nodes it encounters. These nodes continue to forward the message to other nodes, and the procedure continues until the message reaches the destination node or expires. In our system model, the situation can be simplified: Node A first forwards the message to the DTN gateway of its current access network, then the gateway forwards the message to all

the connected gateways using the Internet backbone, and finally each gateway forwards the message within its own network.

This technique does not have to manage the user location for successful message delivery as it simply uses flooding for message delivery. If the destination user is unavailable, the messages are stored in the intermediate nodes across the networks. When the destination user becomes available, the message will be delivered only when a contact occurs between the destination and one of the message carriers.

The main advantage of this technique is that it removes the necessity to manage user location, but it has other drawbacks. The main problem with this approach is that, for a large network size, the number of forwarded messages required to deliver one message increases with an increased number of nodes in the network. The message flooding in the network results in increasing the number of lost messages (as to be discussed in Section 3.3). Another problem is the uncertainty of message delivery upon user reconnection, that happens if the user does not come in contact with any of message holders. The message holders may also decide to remove the message due to their limited buffer space before a contact with the destination takes place. As discussed in Section 2.2.1, the hub count can be defined as the number of times that the message is allowed to be forwarded. For this approach, it is crucial to determine a suitable hub count value that achieves the required message delivery rate without exhausting network resources with the unnecessary circulation of forwarded messages. The hub count value should be large enough to guarantee a successful message delivery, which is difficult to achieve for large-size networks.

3.2.2 Centralized Node Scheme

The second possible solution is a centralized routing approach. A server resides on the Internet (as shown in Figure 3.1), and it is able to communicate with all the gateways. Every node upon connecting to the system must inform the server of its current location. When a node wants to send a message, it first contacts the server to find out where the destination node is located, and then tries to establish a direct connection with the destination node. If the path setup fails or the connection drops at any time, all the messages are sent to and stored at the server for retrieval from the destination node upon reconnecting.

Users have to inform the server about their current locations upon connecting. The server can easily locate any user if that user is connected. The main advantage for this technique, over the epidemic based technique, is that it gives the sender and the receiver the option to establish a direct connection. This is important as there may exist an end-to-end path between the communicating nodes. For example, if the sender is connected through a cellular network and the receiver is connected through another cellular network or even a WLAN, a physical end-to-end path can be established in this case. Establishing a physical end-to-end path will reduce the delay resulting from communicating through the server as an intermediate node. The server role in this case is to locate the destination. The importance of the server becomes clear if the destination user is disconnected or the end-to-end path is unavailable. For example, if the sender is connected through a cellular network and the receiver is connected through a sparse mobile ad-hoc network. The messages must go through the server when the destination is not reachable. The server stores the messages and forwards them to the destination when it is connected.

The main problem with this solution is scalability. The server becomes a

bottleneck in the system even for small-size networks. For large-size networks, this solution is not practical at all.

3.2.3 New Architecture with Super Nodes

Our proposed solution is to combine the preceding two approaches to overcome their limitations. Instead of having a single server, a number of servers at fixed locations, referred to as *super nodes*, are used. They are connected over the Internet (not through access networks) and they have fixed IDs. Each super node is responsible for a set of subscribers (*i.e.*, users). Each user (*i.e.*, mobile node) has a unique and fixed super node, independent of its location changes. The communication between a super node and a DTN gateway is assumed to be reliable over the Internet. In fact, a super node can also act as a DTN gateway; in this case, the super node is responsible for message delivery over the wireless access networks for which it acts as a DTN gateway.

To send a message, the source node first locates the super node of the destination node based on user ID hashing. The hashing of user ID can be obtained based on a predefined hash function that should be globally known to all nodes in the system. This hash function is a mapping function, which maps user ID to a super node ID. It should not be confused with cryptographic hash functions. There are several approaches for defining this function and assigning the user ID. One approach is to append the user ID to the super node ID. In this case the hash function extracts the bytes that represent the super node address. For example, assuming 6 bytes ID of a user as 20.30.40.50.10.5, if we assume a maximum number of super nodes of 2^{16}, and the maximum number of users per super node is 2^{32}, we assign the first 2 bytes to represent the super node address and the remaining 4 bytes to represents the node ID within this super node.

The hashing of the user ID, in this case, will result in the ID of the super node as 20.30. Another possible approach is to use a distributed hash table system such as CAN [78]. The selection of an addressing scheme and a proper hashing (*i.e.*, mapping) function is based on the actual system constraints such as the number of nodes and the number of super nodes in the system.

Each mobile node should contact its super node to update its location upon connecting to an access network. With the latest location of the destination node provided by its super node, the source node tries to establish a physical end-to-end connection with the destination. As discussed earlier (in the single server case), this physical end-to-end connection speeds up the communication and relaxes the load over the super node. If the connection setup fails or the connection drops at any time, all the messages are sent to and stored at the destination super node for forwarding to the destination node upon its availability.

The super node may choose to temporarily transfer its custody of a specific user to another super node. This super node is called *custodian super node*. It becomes responsible of that user communication during the custody period. In the case of custody transfer, the main super node forwards requests for the user to the new custodian super node. In our system, the custody transfer can occur for two reasons.

1. *Load balancing:* The load imposed on super nodes can be regarded as the messages received and stored for all the users. These messages impose two types of load: One is storage space load to store these messages during the user unavailability; The other is communication load imposed to deliver these messages to their destinations. The load imposed by each user depends on factors such as the user availability, and the expected volume of messages for the user. Due to differences of the imposed loads

over different super nodes, some super nodes may become overloaded while others may be underloaded. The custody transfer in this case can achieve load balancing among the super nodes in order to efficiently utilize the available resources.

2. *Reducing communication cost:* The home super node may decide to transfer the user custody to another super node that has lower communication cost with the current user access network. For example, assume the main super node for a user resides in Canada, and the user takes a vacation at Paris. If the user messages are sent to the main super node in Canada, the messages need to travel all the way to a gateway in Paris to be delivered to the user. It should be more efficient if the main super node temporarily transfers the custody of user messages to another super node in France for the period of user roaming there. That is, instead of receiving messages for the user and then sending them to France, the main super node will redirect all message senders to the custodian super node.

To better illustrate the super node approach, consider a simple scenario as shown in Figure 3.2. Node A wants to send a message to node B. By hashing the ID of node B, it locates the super node S_B of node B. Node A sends to S_B a query about node B's location. Super node S_B sends to node A a message that contains the last known location and the custodian super node (the current super node on custody of node B messages) of node B. Then, node A tries to establish a direct connection to node B, that may be possible in some cases (*e.g.*, if node B is connected through a WLAN or a cellular network) or may be infeasible (*e.g.*, if node B is connected through a sparse mobile ad-hoc network with an intermittent link). Suppose that node B is connected through the wireless mobile ad-hoc network and its current custodian super node is S_D.

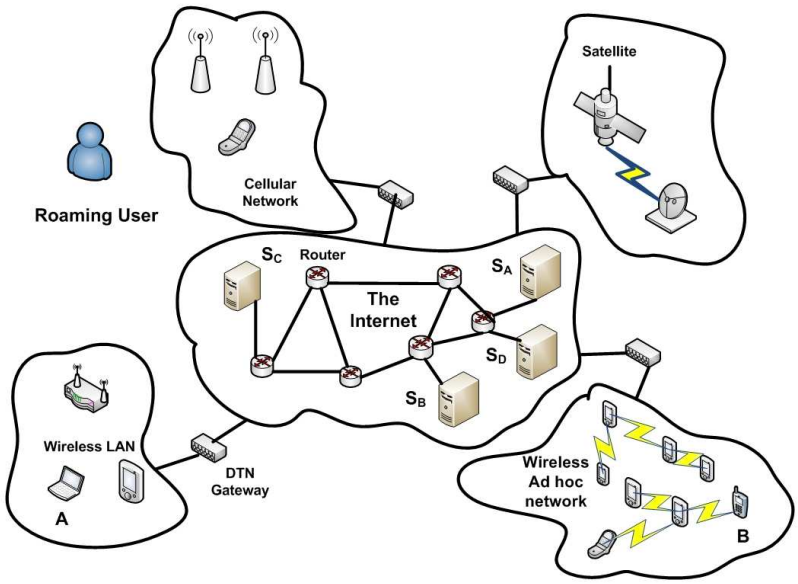

Figure 3.2: The proposed network architecture with super nodes

Node A first tries to establish a connection with node B directly, but fails; then node A sends the messages to super node S_D. It is S_D's responsibility to deliver the messages to node B over the access network. If node B is disconnected from an access network in custody by super node S_D, then S_D will send the stored messages back to node B's permanent super node S_B. Afterward, super node S_B updates its record, declares itself the current custodian super node for B. When node B informs S_B of its current network upon its reconnection, super node S_B will transfer the stored messages and custody to the new custodian super node of node B based on node B's current access network. Due to an expected intermittent connection between node B and its current access network, there may be bounced messages due to the custody transfer. To prevent message bouncing, the custodian super node does not transfer the custody until a timeout period that depends on the access network nature and the load on that custodian

super node. If the custody is not transferred and S_B finds that B is connected via an access network not in jurisdiction of the current custodian super node, the permanent super node S_B will inform the current custodian to transfer the custody to the new custodian (i.e. the super node in custody of the new access network).

It should be noted that the number of super nodes in the system is not dependent on the number of the access networks (unless a super node also functions as the gateway of the access network). The number of the super nodes should be a function of the number of the users in the system. This function can be defined based on the cost induced of assigning a specific node to a super node. This cost is defined as the sum of the buffer space cost required to buffer messages for the node, and the communication cost to deliver the messages from the super node to the node (*e.g.*, the communication path can involve multiple carriers with different network charges). The number of super nodes should be chosen to minimize the cost while making efficient utilization of the super node resources (*i.e.*, communication bandwidth and buffer space). This topic needs further research as it is considered a part of the problem of achieving load balance (discussed in Section 7.2). In this thesis, we consider the cost of assigning a node to a super node is the same for all the nodes and all the super nodes. As a result, the number of super node is a function of the number of nodes and each super node can take up to a maximum number of nodes assigned statically. The centralized node scheme can be regarded as a special case of the super node scheme that suits a very small number of users.

The super node system reliability is defined as the system ability to deliver a message even if its destination is not available, given that the destination can be contacted within the message lifetime.

3.3 Performance Evaluation

3.3.1 Simulation

We use a discrete event simulator written in visual C sharp and MATLAB. The simulation proceeds for a specified number of simulation steps determined by the simulation duration parameter. A summary of all the simulation parameters is given in Table 3.1. The simulation scripts are tested using scenarios with pre-calculated results. Each simulation experiment is repeated for 10 independent runs. The variation in simulation results among these simulation runs was not statistically significant. At the end of the simulation runs, all the log files are processed by a MATLAB script and the results averaged over the 10 runs are plotted on graphs. Each simulation experiment is repeated under the different message delivery schemes (*i.e.*, super node scheme and the epidemic based scheme) and the results are compared. Further simulation details are given in Appendix B.

3.3.2 Simulation Results

We compare the performance of routing based on the super node architecture with the epidemic routing based scheme. The performance is measured in terms of the number of exchanged messages over the network to capture how efficiently each scheme uses the available resources such as radio bandwidth, and the number of undelivered messages to indicate how successful the scheme is in delivering messages.

In our experiments, the system has 4 super nodes, 5 wireless access networks (*i.e.*, 3 sparse mobile ad-hoc networks, 1 WLAN, and 1 cellular network) each connected via its own gateway to the Internet backbone, and $50 - 100$ mobile

Table 3.1: Simulation parameters.

Parameter	Value
Simulation duration	3000 *steps*
Node buffer	20 $Messages$
Number of nodes	$50 - 100$
Probability to connect to the previous network upon reconnection	0.7
Probability to connect to a different network upon reconnection	0.3
Gateway buffer space	2000 *messages*
Super node buffer space	2000 *messages*
Time to collect statistics	100 *steps*
Message TTL	4 *steps*
Number of partitions for MANET	100
Number of message transfers per simulation step	40
Network mean residence time	10 *steps*
Mean disconnection time	10 *steps*
Number of super nodes	4
Number of gateways	5
Number of WLANs	1
Number of cellular networks	1
Node speed	1 $partition/step$
Number of MANETs	3

nodes distributed randomly within the access networks. Each super node is assigned an equal number of users. A user can roam over all the access networks, the residence time over each network being an exponentially distributed random variable with mean of 10 simulation steps. Each user is disconnected for a random period of time (which is an exponential random variable with mean of 10 simulation steps), then reconnected either from the same access network (with probability 0.7) or from any other access network equally likely. All the messages are equal in size, with the same message time to live (TTL) of 4 simulation steps. The buffer space is 20 messages at each mobile node and 2000 messages at each super node and each gateway.

For simplicity in simulation, we use the epidemic routing over mobile ad-hoc networks. For each experiment, a communication scenario (i.e., set of messages, user movements, user disconnections and reconnections events) is set up randomly and run for each scheme.

Figure 3.3 shows the total number of message exchanges for networks with 50 and 100 mobile nodes respectively. It is clear that the super nodes scheme outperforms the epidemic routing based scheme, requiring a much smaller overhead for message exchanges for successful message transfer. Unlike the epidemic routing based scheme, the super nodes scheme does not need to send the messages over all the networks, but only to the current access network of the destination node. It is noted that the performance improvement of using the super nodes scheme, in terms of the number of exchanged messages and the number of lost messages, increases when the network size increases (represented by the number of mobile nodes here). On the other hand, the super nodes scheme still requires many message exchanges. This is because the majority of the access networks, in our simulation, are mobile ad-hoc networks, and message delivery over mobile ad-hoc network requires the exchange of many messages when us-

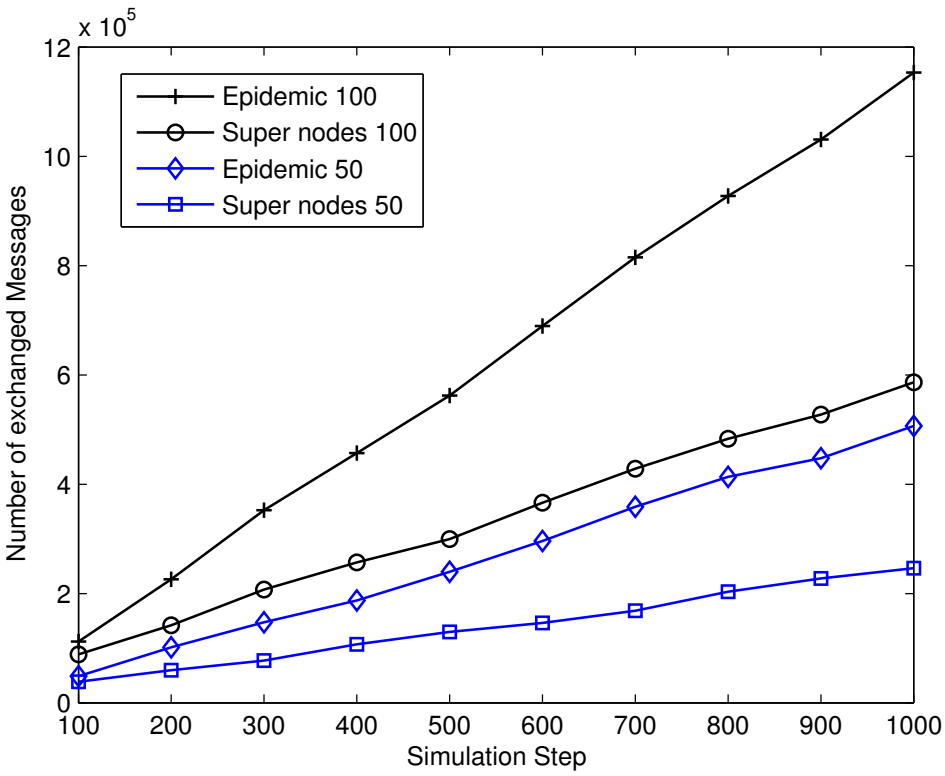

Figure 3.3: The total number of exchanged messages.

ing the epidemic routing within each ad-hoc network. We address this problem with a novel routing approach, introduced in Chapter 4, that reduces the required number of message exchanges while maintaining acceptable performance in terms of the number of undelivered messages.

Figure 3.4 shows the number of undelivered messages. It is observed that the super nodes scheme gives much better performance in terms of the number of undelivered messages when compared with the epidemic routing based scheme. The main problem with the epidemic routing based scheme is that every message is forwarded to all possible intermediate mobile nodes which some of them may never meet the destination node. With the increasing number of messages,

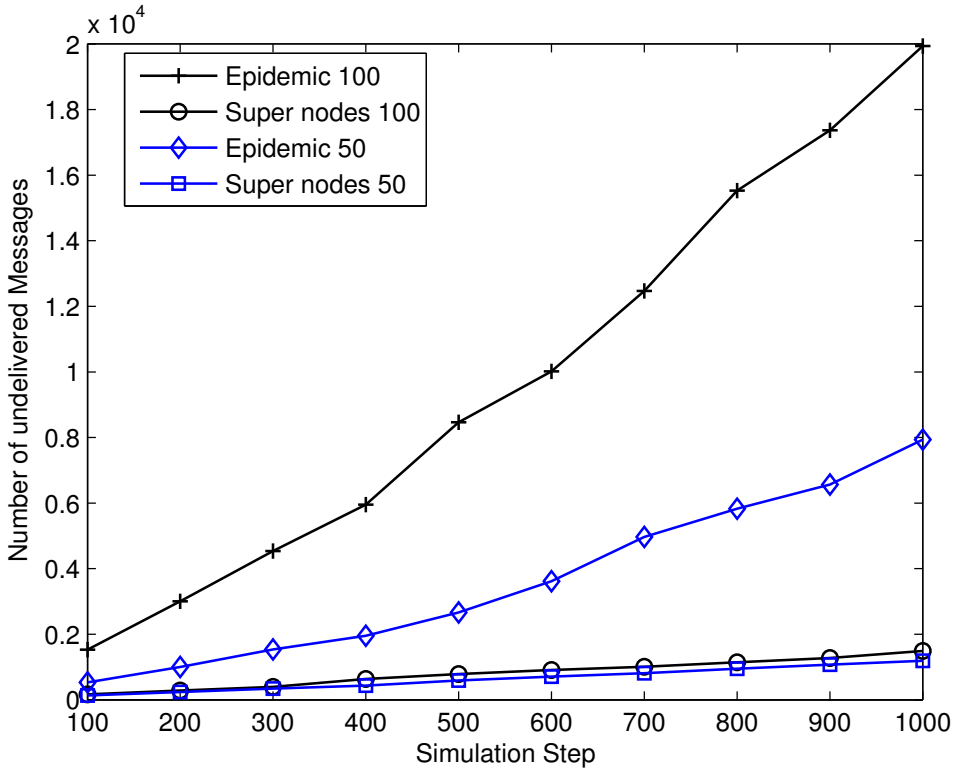

Figure 3.4: The number of undelivered messages.

intermediate nodes may have to drop some carried messages due to the buffer space limitation, resulting in undelivered messages. It is obvious from the figure that the number of undelivered messages is affected by the number of the mobile nodes in the system. This is mainly because increasing the number of nodes results in increasing the number of circulating messages. On the other hand, for the super nodes scheme, the messages are kept at the super node buffer until the destination nodes are reconnected. Hence, message loss is mainly due to the message time to live (TTL) (*i.e.*, the message expired before its destination node is located over the network). Increasing the message time to live (TTL) decreases the number of the undelivered messages, but also increases

the required buffer space at the super nodes. The change of the network size (as the number of mobile nodes is increased from 50 to 100) slightly increases the number of undelivered messages, because it mainly depends on the super node buffer size but not the buffer size at each mobile node.

3.4 Some Related Work

There exist related schemes to handle communications with roaming users, such as in the terminodes project [79], yet they do not handle the potential intermittent connections of the users. The terminodes project is proposed to construct a huge self-organized network of mobile nodes. It is assumed that, with a large number of nodes, the node density is high. As a result, an end-to-end path is likely to exist between two communicating nodes. However, the super node architecture is concerned with the interconnection of heterogeneous wireless access networks to provide a virtually continuous connection for a roaming user over the networks (*e.g.*, cellular networks, MANETs, and WLANs). For MANETs within the super node system, it is assumed that the networks can be sparse so that an end-to-end path between nodes within the network is unlikely. Communications in terminodes are based on assigning each node with a virtual home region (VHR). Each node should determine its geographical location and send this information back to all the nodes within its VHR. Any node wishing to communicate with this node should determine its location by contacting any node within its VHR and then forward its messages to this location. However, applying the technique to solve the problem under study in our research raises many issues: First, without availability of the destination node, the communication will not take place and/or the messages will be lost; Second, with the potential unreliability of the participating nodes, the node location information

is not guaranteed to be stored reliably within the VHR; Third, due to the potential unreliable communication between nodes within the VHR, the location information stored within the nodes in VHR may be inconsistent; Finally, the VHR may happen to be empty of nodes at any time, which prevents the communication with all the associated nodes to be located. On the other hand, the super node architecture solves these issues by replacing the VHR with a reliable super node residing in the Internet, which acts as a communication delegate for the node, so that even with unavailability of the node itself the message delivery to the super node can still take place.

The super node architecture can be regarded as an adaptation of the super node concept in peer-to-peer networks (where a super node plays a special network role for regular peers [80]) to the DTN domain. There is much similarity between the peer-to-peer systems with the DTN in general such as using peer-to-peer reputation systems [81–84] for coping with node cooperation over the network [85–87]. However, DTNs address problems and system constraints that are different from that of peer-to-peer systems, where peer-to-peer systems can be generally regarded from the application layer perspective [88, 89].

3.5 Summary

In this chapter, we present the system model and our research problem of how to achieve connectivity to roaming users with intermittent connections over heterogeneous terrestrial wireless access networks. Based on the store-and-forward strategy used in DTNs, we discuss three possible solutions to the problem. The main solution is based on the idea of using super nodes as roaming node delegates. We discussed various aspects of the proposed techniques such as node addressing. We conducted a simulation study to evaluate the performance of

the super nodes scheme and the epidemic routing based scheme. The simulation demonstrates that the super nodes based solution outperforms the epidemic based solution, especially for large networks, in terms of message exchange overhead and the number of lost messages.

Chapter 4

Reliable Message Routing in MANETs

Message delivery process over the super nodes system can be regarded as a consecutive number of phases. An end user sends a message that is routed over the user's current access network to the network gateway. The gateway forwards the message to the destination user's super node over the Internet backbone. The super node then forwards the message to the gateway of the destination user's access network based on the user current location. Finally, the gateway routes the message over the network to its destination. As a result, routing over the proposed super node system can be regarded on two levels. The first level is routing among gateways and super nodes. The second level is routing between the end user and the network gateway over the user's current access network.

Based on the super nodes system model, communication among super nodes and gateways is assumed to be reliable over the Internet backbone. The super nodes and gateways are assumed to have fixed network locations over the Internet. As a result, message routing among super nodes and gateways can base on

the regular Internet routing. On the other hand, user roaming and intermittent connection impose many challenges for reliable message routing over wireless access networks. No routing technique can be generalized for all the wireless access networks as each network faces different challenges based on its type. Wireless access networks can be regarded within two general categories, infrastructure based networks and infrastructure-less networks. For infrastructure based networks (*e.g.*, cellular networks, and WLANs), current regular routing techniques can be applied with minor modifications to deliver a message when the destination user is available. For example, in cellular networks, successful message delivery can be achieved by forwarding the message to the base station through which the destination user is currently connected. On the other hand, routing becomes more complicated for infrastructure-less networks (*e.g.*, MANETs), due to the potential unavailability of a physical end-to-end path between the gateway and the destination user over such type of networks.

Our research focus is how to cope with routing challenges over infrastructure-less networks in general and on MANETs in particular. MANETs are considered an essential component of wireless access networks in the super nodes system. They can provide service coverage over areas where there is no network infrastructure to provide communication services. Integrating MANETs as part of the super nodes system introduces many challenges such as preventing unauthorized use of the networks and achieving end-to-end message security that are studied in Chapter 6. One main challenge is how to route a message over a MANET. We present a new routing technique [5, 6] for challenged mobile ad-hoc networks based on the store and forward mechanism employed by the DTN system architecture. Our contributions are three-fold: (i) We introduce a concept of *virtual network topology*, which is a redefinition of the network topology concept to match the DTN context; (ii) we propose a new approach based on

contact time duration for calculating the probability of future contacts in DTN networks; (iii) we present a new routing technique that is based on calculating a dominating set for the virtual network topology, using a new algorithm for dominating set calculations.

4.1 The MANET System Model

The system model for the MANET under consideration is regarded as a part of the super nodes system. Here, we consider a MANET as an access network that provides connection to roaming users over the super nodes system. The network coverage is limited by a geographical area. In the area resides a DTN gateway which connects the access network (*i.e.*, MANET) to the super nodes system using the Internet backbone. Within the MANET, there are a number of mobile nodes that can freely roam over the network coverage area. These nodes may have different communication capabilities in terms of wireless transmission range, memory size, and available transmission power. The nodes are free to enter or leave the area and consequently join or leave the network. A node can be unreliable because it can switch off at any time with or without a warning.

Figure 4.1 illustrates a schematic diagram for the MANET model. The DTN gateway provides connectivity through the Internet backbone. Nodes are roaming freely over the area covered by the network. The nodes are free to enter the area covered by the network such as node E or leave the area such node D. Two nodes are connected when they are able to communicate with each other (*i.e.*, when they are within each other's transmission range). For simplicity, we assume that all nodes have the same transmission range, and that if a node, A, can receive a message from node, C, then node C can receive from node A as well. We are interested in a situation where the mobile nodes are sparsely

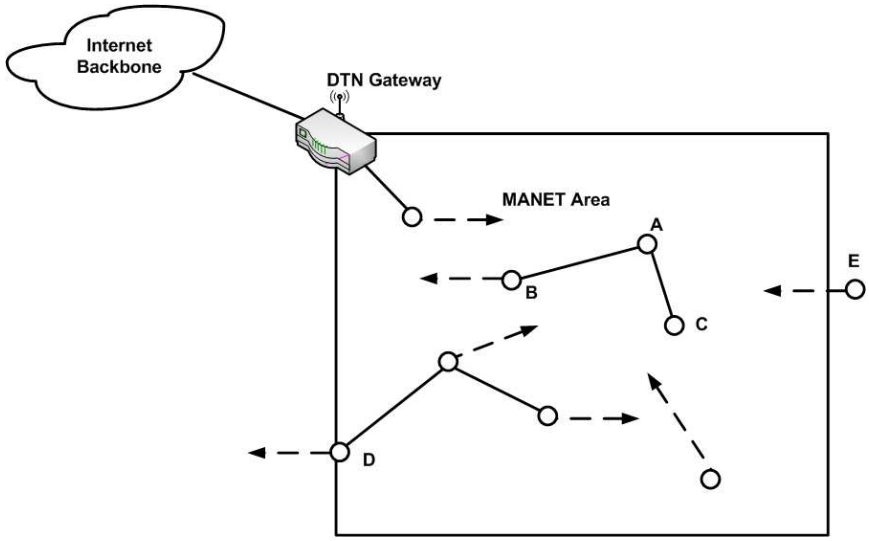

Figure 4.1: An illustration of the MANET under consideration.

located and the network is very likely to be partitioned, such that an end-to-end path between a pair of communicating nodes is very rare.

The DTN gateway has a fixed location within the geographical area, with communication functions and capabilities similar to those of an ordinary mobile node. That is, the gateway is assumed to have a limited transmission range, and can communicate only with the nodes within its transmission range. The gateway transmission range covers only a small portion of the MANET geographical area. On the other hand, the gateway has higher processing power and larger storage (buffer) space than other roaming nodes. In terms of node mobility pattern, there is no restriction on node movements (except a reasonable upper bound on the velocity). An assumption is that some nodes usually roam toward the gateway, so that the gateway can communicate with the roaming nodes from time to time. This assumption can be satisfied by carefully choosing the gateway location, depending on the geographical features of the service

coverage area.

4.1.1 Node Mobility Model

As real life users usually follow specific patterns in their movements, we consider the following user mobility model.

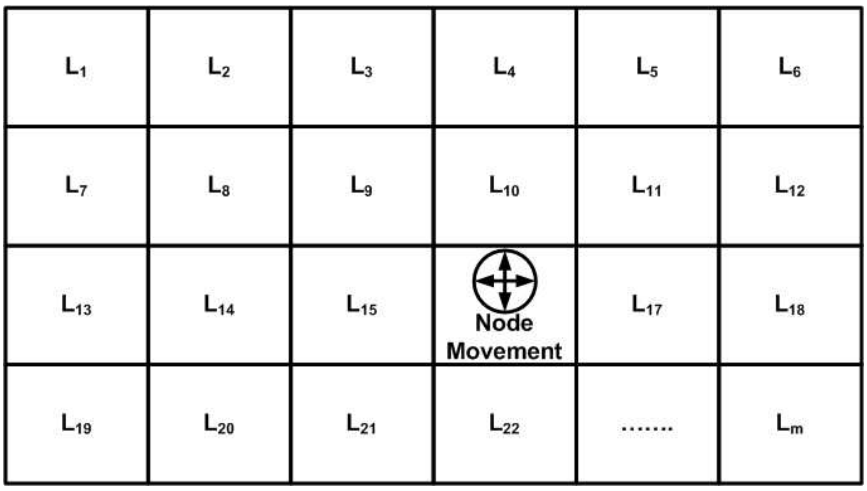

Figure 4.2: Network partitioning and user movement.

The geographical area covered by the MANET is partitioned to m partitions as shown in Figure 4.2. When a node is connected to the network, it visits each of the partitions with a certain probability. The location of a mobile node in the future is independent of its location in the past, given its current location. Denote the location state of a mobile node by the partition it resides, and assume the residence times of all the mobile nodes in each partition are iid exponential random variables. Then the user mobility model can be characterized by a one-dimensional Markov chain, with location state space $\{L_1, L_2, \ldots, L_m\}$, as shown in Figure 4.3.

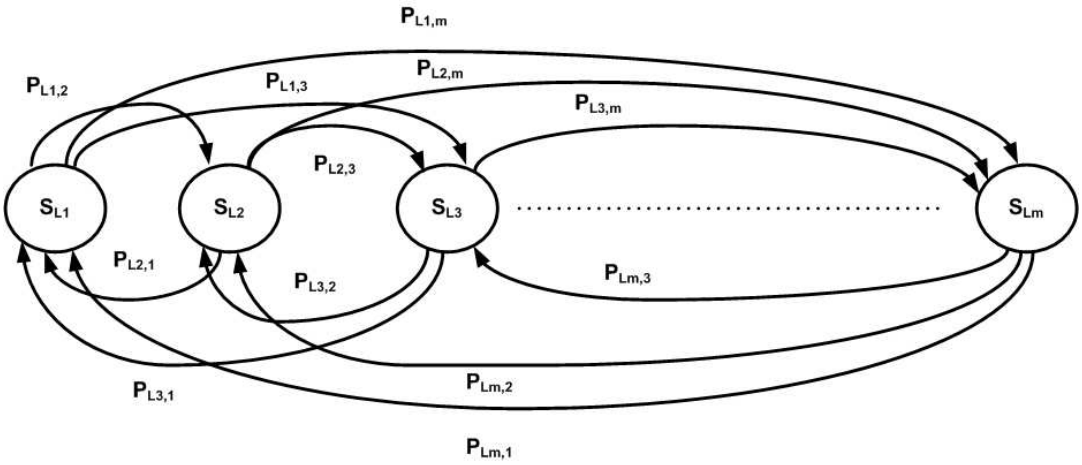

Figure 4.3: Modeling of user movement by a finite-state Markov chain.

The user movement model over the network coverage area is described by the transition matrix $\mathbb{M}$ of the Markov chain, given by

$$\mathbb{M} = \begin{pmatrix} P_{L_{1,1}} & P_{L_{1,2}} & \dots & P_{L_{1,m}} \\ P_{L_{2,1}} & P_{L_{2,2}} & \dots & P_{L_{2,m}} \\ \dots & \dots & \dots & \dots \\ P_{L_{m,1}} & P_{L_{m,2}} & \dots & P_{L_{m,m}} \end{pmatrix} \tag{4.1}$$

where $P_{L_{i,j}}$ is the conditional probability that a mobile node will enter partition L_j given that it is still connected to the network and it leaves its current partition L_i. For any partition L_i, we have $\sum_j P_{L_{i,j}} = 1$. The transition probability matrix depends on the geographical characteristics of the service area and the network environment under study.

4.2 Previous Routing over MANET

Integrating MANETs as part of the super node system introduces many challenges in order to achieve seamless message delivery for roaming users. There

exist various regular routing techniques, such as AODV [32], DSR [35] and DSDV [38]. The idea of routing in ad-hoc networks based on calculating the minimum connected dominating set is introduced in [90]. The main limitation of the regular MANET routing schemes is the need for an end-to-end path between the source and the destination, which makes them unsuitable for the system under consideration.

Research efforts have been devoted to routing in a sparse mobile ad-hoc network (*e.g.*, [44, 45]), which depends on known routes and movements of some nodes to deliver messages. Moreover, a moving node may be required to change its movement trajectory to deliver a message [41]. Some routing schemes require to collect information from the moving nodes about their destination, velocity and direction of movement, which requires much computations and the awareness of destination node locations to find the best moving node(s) to carry messages. That is, these techniques make routing decisions based on a pre-known moving schedule of the mobile nodes. Other techniques assume totally scheduled contacts among nodes [62, 63]. The existing schemes are not suitable for the MANET of interest where mobile nodes move randomly (freely) without known schedule. On the other hand, epidemic routing [58] assumes no knowledge about the network topology. It uses flooding to deliver messages, each node forwards its received message to all its neighbor nodes. The message delivery mainly depends on node mobility, taking advantage that one of the message carriers may meet the message's destination node. Therefore, it is inefficient in terms of resources utilization, but sometimes necessary. A compromise between the two extremes is routing based on prediction of the future movement of a node using the knowledge of its previous location and movement pattern [42, 65]. The previous work predicts future contacts based on the number of previous contacts, which suffers from some deficiency that

will be discussed Section 4.4. To overcome the inadequacy, we propose here a time-based method for estimating the probability of future contacts.

4.3 Virtual Network Topology for MANET

To route a message is to find a path from the traffic source to send this message to its destination. For the challenged network scenario that we are interested in, it is difficult, if not impossible, to find such a path. MANET routing algorithms depend mainly on constructing the network topology and then processing this topology to find a path (or paths). These algorithms require that each node has a full or partial knowledge of the network topology. Constructing and maintaining this kind of topology in our case means unnecessary overhead as the network is expected to be sparse most of the time. Furthermore, these algorithms fail if there is no end-to-end path between the source and destination nodes, which can happen with a high probability.

Our approach to address the routing issue is to construct a virtual network topology, where a link between two mobile nodes represents the probability of future contacts (*i.e.*, meetings) between the two nodes within the network, instead of representing the existing physical connection between the nodes. A *contact* is defined as an opportunity of transmitting and receiving data between two nodes as they fall within each other's transmission range.

As shown in Figure 4.4, a simple network is represented as an undirected graph $G = (V, E)$, where V represents the set of mobile nodes *currently* participating in the network and E represents the set of contact probabilities for all node pairs. Note that Figure 4.4 illustrates only the links having a nonzero probability of future contacts.

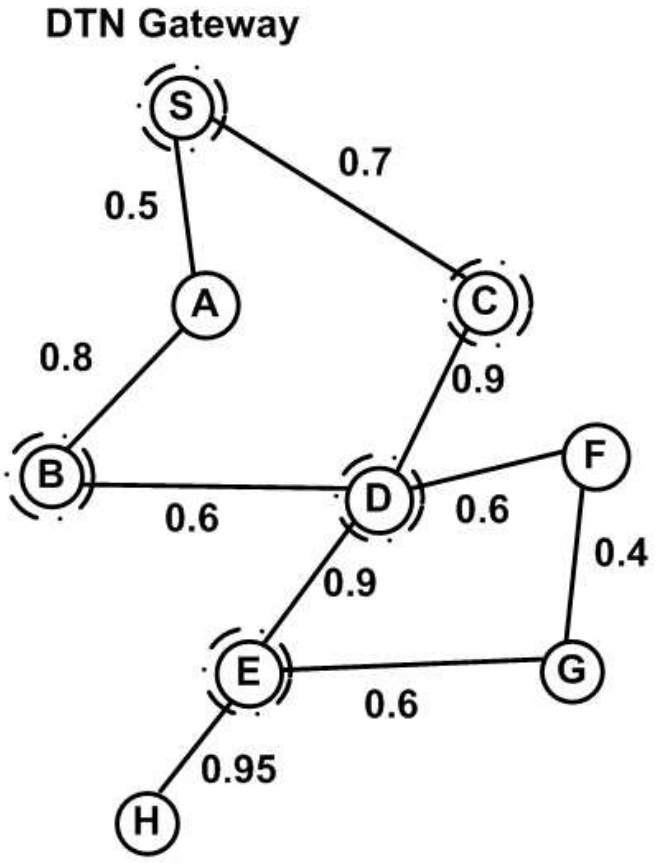

Figure 4.4: A simple example of virtual network topology.

4.4 Probability of Future Contacts

The main challenge in developing an efficient routing algorithm for the MANET, under consideration, is how to construct the *virtual network topology*, *i.e.*, how to calculate the probability of future contacts between a pair of nodes. Techniques proposed for DTN routing use different criteria for predicting future contacts, *e.g.*, the idea that a most recently met node is more probably to be met [65]. Some techniques assume that each user has a predefined movement pattern that

rarely changes and the routing decisions are based on these patterns [67]. Other techniques assume that the future events in the network are known in advance, which is unreasonable for our system where mobile users roam freely anytime and anywhere.

There is no general solution to the problem; however, a proper solution mainly depends on network constraints. Here, the system under consideration does not have any knowledge of the future events (*e.g.*, node velocity, node movement direction, time instants of power on and off). Instead, we make use of network statistics that are collected and stored on the DTN gateway. The statistics are collected based on all the user sessions in the access network in the system, not only the current or most recent session.

Previous techniques [42, 65] predict future contacts based on the number of previous contacts. Such an approach has two problems: One is multiple *falsely detected contacts*, as shown in Figure 4.5, where a node, B, is in the communication range of a node, A. As node B may switch its power off and then switch it back on, node A will falsely detect more than one contact with node B. The same situation can happen when node B exhibits an intermittent connection with node A, *e.g.*, due a communication barrier between them or the presence of node B on the edge of node A's communication range.

The other problem is related to *permanent neighbors*, as shown in Figure 4.5 where a node, C, and a node, D, move with the same velocity and in the same direction. One contact between the two nodes would be counted because no disconnection happens, independent of the long duration that the contact lasts. On the other hand, both nodes encounter other nodes as they move, which can result in multiple contacts for these nodes due to on and off links. A routing decision based on the number of contacts makes node C a less suitable candidate to carry message for node D than other nodes having a larger

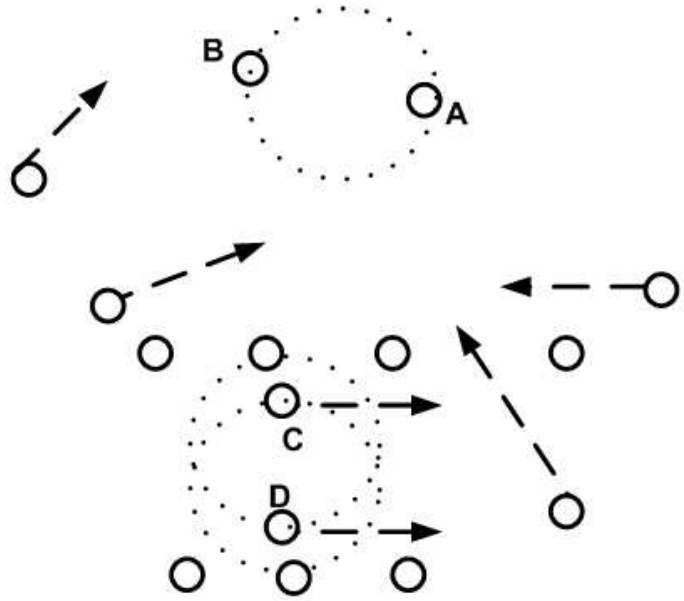

Figure 4.5: Problems with using the number of contacts as a parameter.

number of contacts, although node C should be an optimal candidate to carry the messages as it is in continuous contact with D.

To address the problems, we propose routing based on the durations of previous contacts, instead of the number of previous contacts. Taking the total duration of all the contacts as the parameter is expected to give a better reflection of the likelihood that the nodes are in contact with each other. Without loss of generality, consider two nodes, A and B. At any time, let T_{AB} denote the total time that node A and B were in contact up to the moment. Regardless of time synchronization and the time durations that nodes A and B respectively stayed connected to the network, $T_{AB} = T_{BA}$. The probability of a future

contact between nodes A and B is estimated approximately by

$$P_{AB} = \frac{T_{AB}}{[T_A + T_B]/2} \tag{4.2}$$

where T_A and T_B are the total time durations that nodes A and B respectively connected to the network up to the moment of estimation.

The previous techniques do not take into account the actual duration of node connection to the network. As a result, the probability of contacts decreases with time if no contact occurs even if one or both of the nodes were not connected prior to the time of estimation. The assumption that a node is always on and connected is not practical for our system. On the other hand, Equation (4.2) captures the actual duration that both nodes are connected to the network. The probability of contact, P_{AB} decreases as T_A and/or T_B increases for a given T_{AB}, which means that either node A and/or node B has been connected to the network without encountering each other. On the other hand, the time that both nodes were actually connected to the network simultaneously can be approximated by the minimum of the durations that the nodes were connected to the network respectively, which lead to an alternative estimation given by

$$P_{AB} = \frac{T_{AB}}{min(T_A, T_B)}. \tag{4.3}$$

Each node in the network keeps a list that contains the total duration of the meetings for each encountered node. The node sends this list to the gateway the first time it connects to the network. During the node life time in the network, it sends updates of the list to the gateway by piggyback on regular messages, or by sending special update messages if no regular messages will be sent.

4.5 DTN Dominating-Set Based Routing: Duration based Prediction

Our newly proposed routing scheme [5, 6] is based on calculating a connected dominating set for the virtual network topology graph. A dominating set of a graph is defined as the subset of vertices of the graph where every vertex not in the subset is adjacent to at least one vertex in the subset [90]. In our routing scheme for the MANET, the formulation of the virtual network topology and the determination of its dominating set takes place at the gateway. The results are broadcast to all the mobile nodes in the network via the epidemic routing. That is, the gateway sends the information to all the nodes it encounters. These nodes, during their movements, forward the message to all other contacted nodes. The procedure continues until the information reaches all the mobile nodes in the network. On the other hand, for routing of a data packet from the source node to the destination node, the packet is forwarded only to the nodes in the dominating set, different from the epidemic routing for the message broadcasting. When a node is to send a message, it either transmits it to a node in the dominating set or to the destination node itself (if there is a direct contact).

The epidemic routing based on forwarding the message to all the neighboring nodes, in anticipation that one of these nodes may meet with the destination node in the near future as it roams. On the other hand, our proposed technique counts on forwarding the message to the dominating set members only. The dominating set represents the set of nodes that have high probability to meet with all the other nodes in the network; the expected number of forwarded messages is proportional to the size of the dominating set.

To determine the dominating set, the technique given in [90] is not suitable to our virtual network topology. We should take the edge weights (*i.e.*, the probabilities of future contacts) into consideration, as we may have a fully connected graph where most of the edges have a very low weight. Our procedure for formulating the dominating set contains two phases. In the first phase, for each node not already in the set, we add the node that it is most probable to meet to the dominating set. We process the nodes in ascending order of their ID. The second phase ensures that the dominating set is connected. The dominating set connectivity means that nodes within the set are probable to meet. This is necessary to ensure proper forwarding of a message among the dominating set members in order to deliver it to its destination. As the gateway connects the MANET to the overall system, it should always be included in the dominating set.

Algorithm 4.1 shows the details of our proposed algorithm where DS represents the dominating-set and $NG(i)$ represents the set of neighbors for node i.

As an example to explain the algorithm, consider the simple virtual network topology in Figure 4.4. After constructing the virtual network topology based on the future contact probability information based on previous contact duration, the procedure to determine the dominating set starts as follows. First, we start with the DS containing only the gateway node, S. Processing node A adds node B to the DS. As node B is now an element of DS, it is not processed. Processing node C adds node D to the DS. Processing node E and node F would add node D which is already in the DS. Processing node G adds node E to the DS. Note that node H will not be processed as all its neighbors are already in the DS. After the first phase, $DS = \{S,\ B,\ D,\ E\}$. The second phase finds that the DS is not connected as step 8 results in two connected

Algorithm 4.1 Calculating a connected dominating set (DS) based on previous contact duration

Data: $G = (V, E)$: Virtual network topology connected weighted graph;

V: set of nodes;

E: set of contacts probabilities between node pairs;

Result: DS : set represents the calculated dominating set;

1: Start with DS contains only the gateway node
2: **for all** node $i \in V and\ i \notin DS\ and\ \{NG(i) \cap DS\} \neq NG(i)$ **do**
3: get max P_{ij} where $j \in NG(i)\ and\ NG(j) \backslash \{i\} \neq \phi$
4: **if** $j \notin DS$ **then**
5: add j to DS
6: **end if**
7: **end for**
8: Get connected components in DS by recursively connecting each node $i \in DS$ with node j *where* $j \in NG(i)$ *and* $j \in DS$
9: **if** step 8 results in more than one connected components **then**
10: Select 2 components and find shortest path with highest sum of weights connecting them over the graph G
11: **for all** node i in the calculated path **do**
12: **if** $i \notin DS$ **then**
13: Add node i to DS
14: **end if**
15: **end for**
16: GOTO step 8
17: **end if**

components. The first contains the gateway $\{S\}$ and the second contains the nodes $\{B, D, E\}$. Searching for a shortest path connecting the two components with the highest sum of edge weights will result in the path $\{S, C, D\}$. As a result, Node C is added to DS. The final calculated connected dominating set $DS = \{S, B, D, E, C\}$.

The proposed algorithm results in a dominating set such that each node in the network has a high probability to meet with one or more of the set members. However, the proposed algorithm does not consider the size of the resultant dominating set. Reducing the dominating set size will reduce the number of exchanged messages. Moreover, the construction of the virtual network topology is based on estimating the probability from previous contact duration statistics. Chapter 5 presents another way of estimating the probability of contacts and how to reduce the dominating set size.

4.6 Performance Evaluation

We extend the discrete event simulator described in Section 3.3.1 to simulate the MANET model under consideration. We further use this extended simulator for the experiments in this chapter and following chapters to test the performance of the different proposed approaches. The main change is that we simulate only one MANET with node movements following the mobility model introduced in Section 4.1.1. The updated list of simulation parameters is given in Table 4.1.

We compare the system performance under the newly proposed estimation criterion that uses the previous contact duration with that under the criterion of using the number of previous contacts. Further, We compare the performance of the newly proposed dominating-set based routing technique with that of the epidemic routing. The performance is measured in terms of the number of for-

Table 4.1: Simulation parameters.

Parameter	Value
Simulation duration	3000 *steps*
Number of nodes	$50 - 100$
Node buffer	15 *messages*
Probability to move to a new partition	0.7
Probability to disconnect from network	0.3
Gateway buffer space	2000 *messages*
Time to collect statistics	100 *steps*
Message TTL	40 steps
Number of partitions for MANET	100
Number of message transfers per simulation step	40
Partition mean residence time	20 *steps*
Network mean disconnection time	20 *steps*
Node speed	1 *partition*/*step*
Message generation mean	$\frac{10}{3}$

warded messages over the network to capture how efficiently each technique uses the available resources such as radio bandwidth, and the number of undelivered messages to indicate how successful the technique is in delivering messages (a QoS measure).

In our experiments, the MANET coverage area is a square of size 10×10 partitions. Each simulation proceeds in discrete time steps. Mobile nodes have mobility trajectories independent of each other. We experiment with $50 - 100$ nodes. For each simulation run, a transition matrix $\mathbb{M}$, given by Equation (4.1), is randomly generated and stays fixed till the end of the simulation. Initially, node locations are uniformly distributed over the service area. As the simulation time increases, each node (if connected) moves randomly according to the transition matrix. When a node moves to a new partition, it stays there for a residence time that is an exponential random variable with an average of 20 simulation steps. At the end of the residence time, the node will move to a new partition with a probability of 0.7, or will disconnect from the network with a probability of 0.3. If the node disconnects, it will stay disconnected for a duration that is exponentially distributed with an average of 20 simulation steps. For simplicity, we assume that a node is able to communicate only with the other nodes in the same partition. Messages are generated based on a Poisson process with mean rate of $\frac{10}{3}$ messages per time step. The source and destination mobile nodes for each message are selected at random. All the messages are equal in size, with the same message time to live (TTL) of 40 simulation steps. The buffer space is 15 messages at each mobile node and 2000 messages at the gateway. When the node buffer is full and a new message is received, the oldest message in the buffer is removed to receive the new message. At each time step, the node detects its neighbor nodes and exchanges the buffered messages with them (the messages they do not already have) based on the used routing

technique. Each node also update its buffer by removing the expired messages.

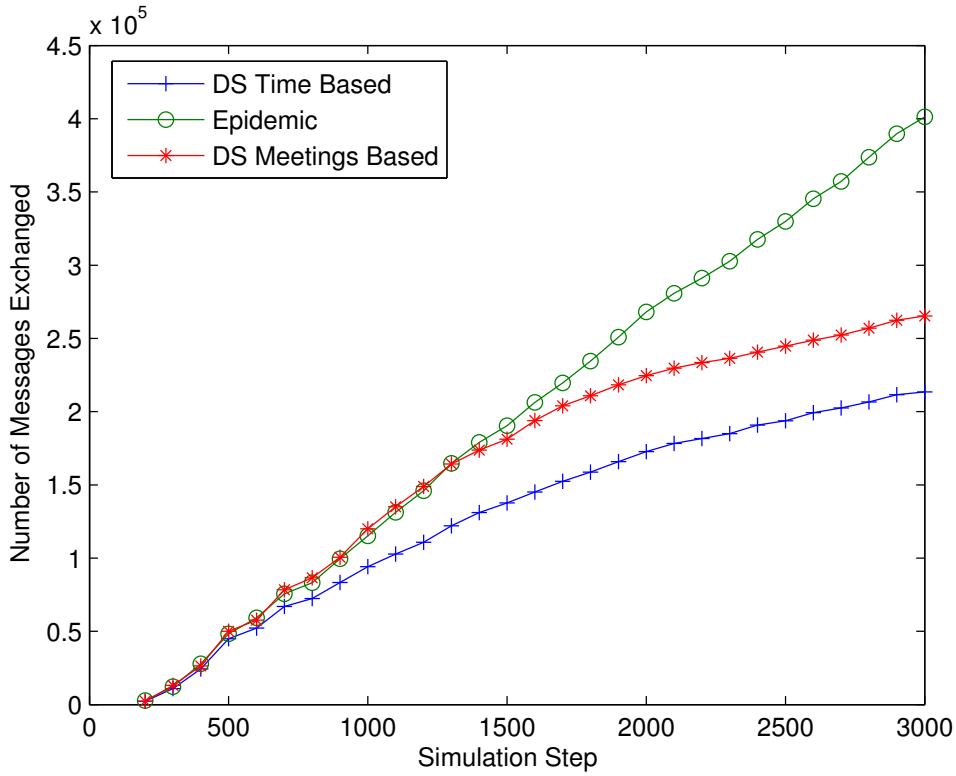

Figure 4.6: Comparison between the epidemic routing and dominating-set based routing with respect to the number of messages exchanged.

For each experiment, a communication scenario (*i.e.*, set of messages, user connections, user disconnections, user movements) is set up randomly and run for each routing technique. In these simulation experiments, we create the condition of near permanent contact between node pairs, as discussed in Section 4.4, by fixing the transition matrix for all network nodes. Moreover, we allow node communications in transitions between partitions and fix the travel path between partition pairs. This results in some nodes will be in long contacts with

other nodes while it is still counted as one contact as discussed in Section 4.4. However, it will be shown in Chapter 5 that even with different mobility matrices for each node the proposed criterion still achieve better performance compared to the epidemic routing. The results we discuss in this section is based on estimating the probability of future contacts based on previous contact duration using Equation 4.2. It is found that using Equation 4.2 and Equation 4.3 for estimating the probability of future contacts based on previous contacts duration give comparable results and the same conclusions when compared with the case of using the number of previous contacts as a metric under our simulation conditions.

Figure 4.6 shows a comparison between the epidemic routing technique and the dominating set based routing technique in terms of the total number of forwarded messages. It includes the results for the dominating-set routing technique based on two different ways of calculating the probability of future contacts. One is based on the number of previous contacts and the other is based on the total contact time as discussed in Section 4.4. It is clear that the dominating set based technique is much better than the epidemic routing in terms of the number of forwarded messages, because in the former scheme each message is forwarded only to the dominating set members, but not all the neighboring nodes as in the latter scheme. It is also observed from the figure that the time based calculation for the dominating set gives better performance than the calculation based on the number of previous contacts.

On the other hand, Figure 4.7 demonstrates that the dominating-set based routing leads to more undelivered messages than the epidemic routing. A message is lost if it has not been delivered to the destination node before the message time to live (TTL) expires. In the new scheme, a message is forwarded only from the dominating set members to the destination, which is more likely to cause

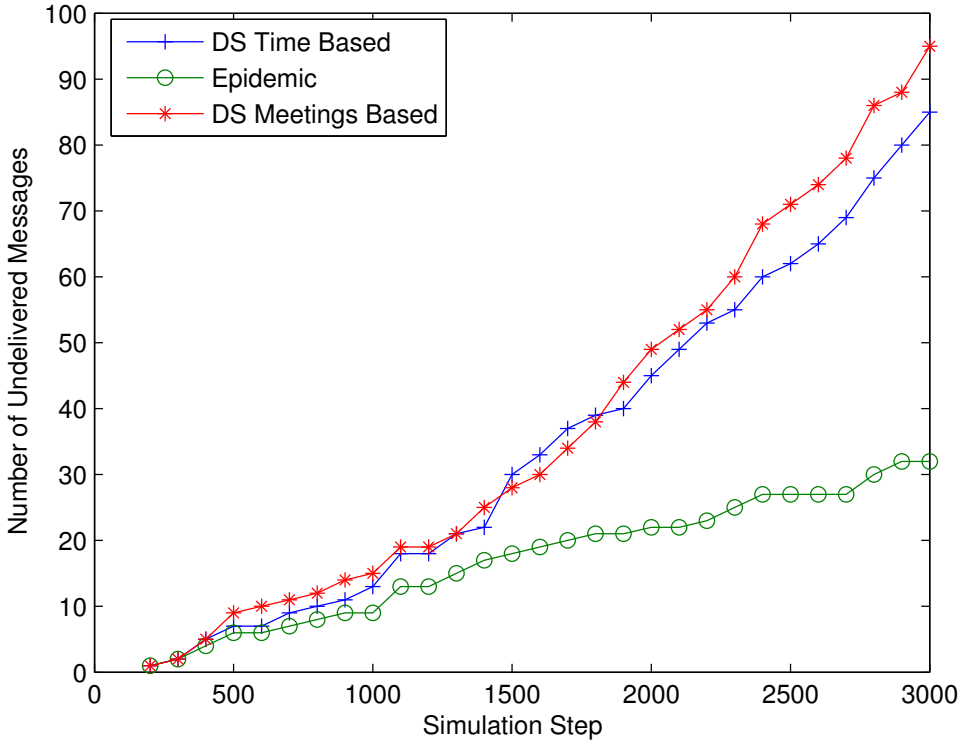

Figure 4.7: Comparison between the epidemic routing and dominating-set based routing with respect to the number of undelivered messages.

a longer delay for the destination node to meet one of the message carriers as compared with the epidemic routing. However, when the message time to live is increased to 80 simulation steps, the two routing schemes give comparable performance in terms of the number of lost messages as shown in Figure 4.8.

Figure 4.7 also shows that calculating the probability of future contacts based on the previous contact durations leads to better routing performance (in terms of the number of undelivered messages) than calculating it based on the number of previous contacts, as the time based probability calculation results

in a more accurate virtual network topology.

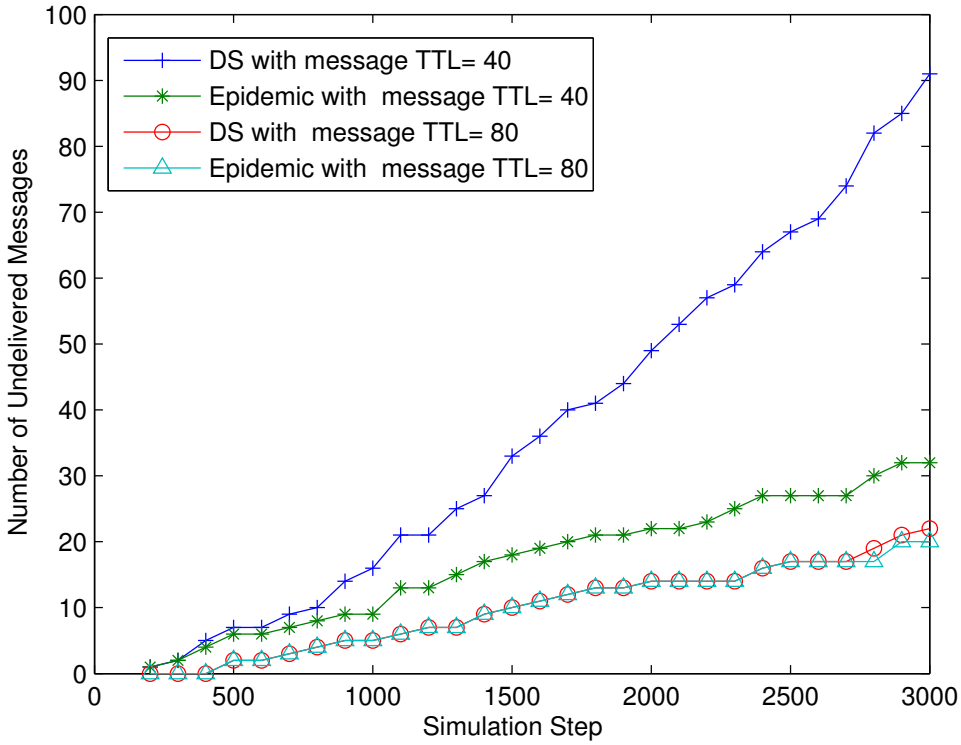

Figure 4.8: Comparison between the epidemic routing and dominating-set based routing with different TTL values in terms of the number of undelivered messages.

Figure 4.8 shows how the message time to live (TTL) affects the number of undelivered messages. Increasing message time to live (TTL) increases message delivery probability as it is more likely that the destination node meets a member in the dominating set. On the other hand, increasing the message TTL increases the number of forwarded messages for both schemes as shown in Figure 4.9, mainly because of the retransmission of dropped messages due to the limited

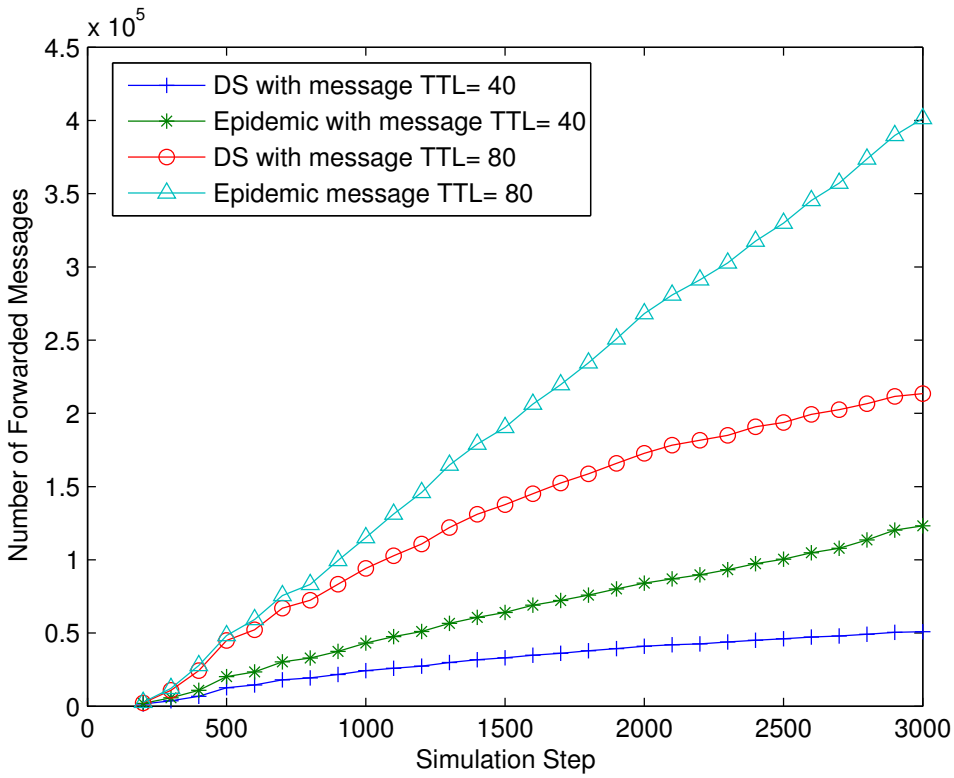

Figure 4.9: Comparison between the epidemic routing and dominating-set based routing with different TTL values in terms of the number of forwarded messages.

buffer space. It is observed that the dominating set routing scheme outperforms, in terms of the number of forwarded messages, the epidemic routing scheme for the different TTL values.

We perform the experiments for different sizes of the network and have the same observations. As shown in Figure 4.10, when the number of nodes is increased to 100, the dominating set routing outperforms the epidemic routing in terms of resource utilization (measured by the number of forwarded messages), and gives comparable performance in terms of the percentage of undelivered

messages. It is noted that, as the MANET operation time increases, the number of forwarded messages decreases as more observation data are available for estimating the probability of future contacts, resulting in a more accurate virtual network topology.

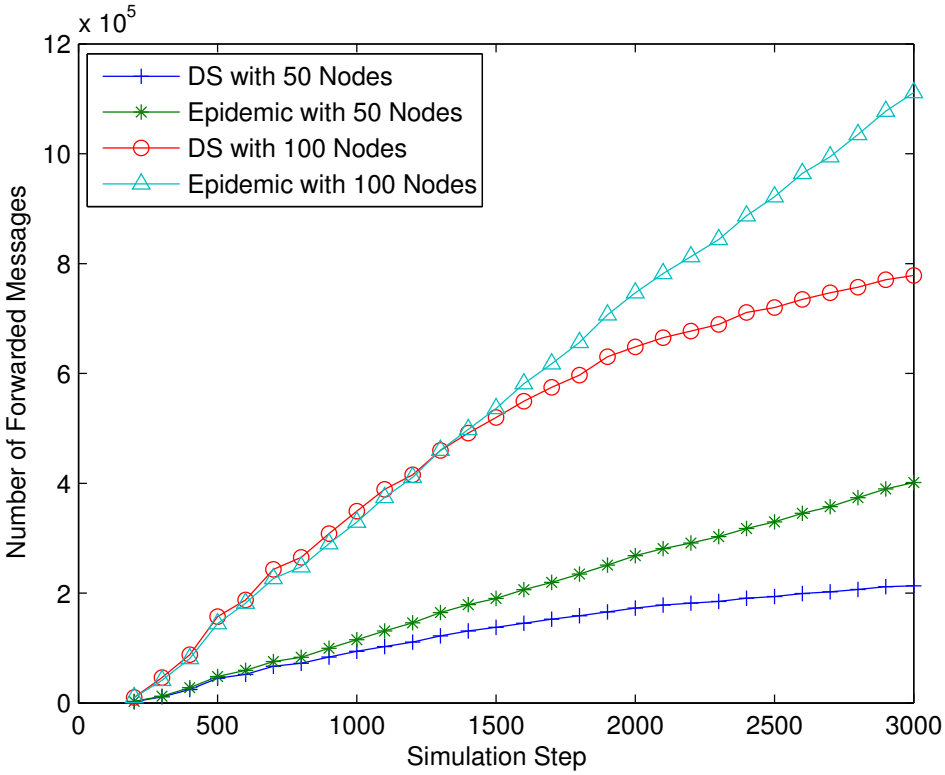

Figure 4.10: Comparison between the epidemic routing and dominating-set based routing with increasing the number of nodes.

Figure 4.11 shows that, as the MANET operation time increases, the dominating set size (*i.e.*, number of nodes) decreases, and a more accurate virtual network topology can be constructed. The figure also shows how the size of the dominating set is dependent on the number of nodes in the network. But, re-

gardless of the network size, the dominating set size decreases with the MANET operation time, which also causes the number of forwarded messages to decrease (as shown in Figure 4.10). As a result, the dominating set routing technique gives better performance when the MANET operation time increases.

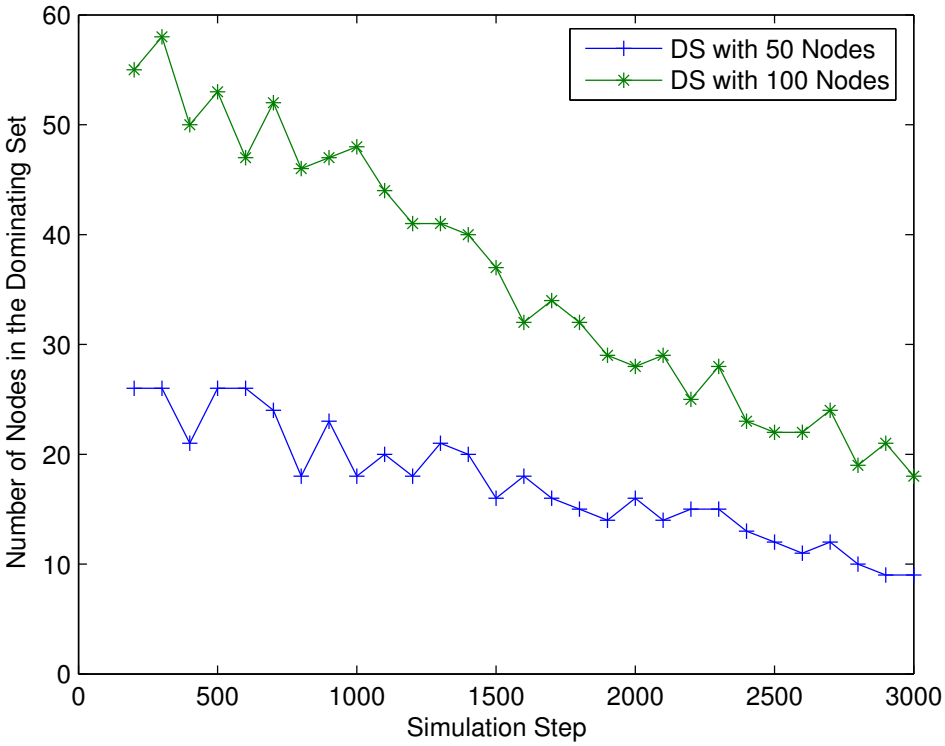

Figure 4.11: The dominating set size.

To study the buffer size effect, we increase the message TTL to 80, so that both schemes have comparable performance in terms of the percentage of undelivered messages. As shown in Figure 4.12, the performance of both routing schemes degrades (in terms of the number of undelivered messages) when the buffer size is reduced, but the dominating-set based routing still outperforms

the epidemic routing.

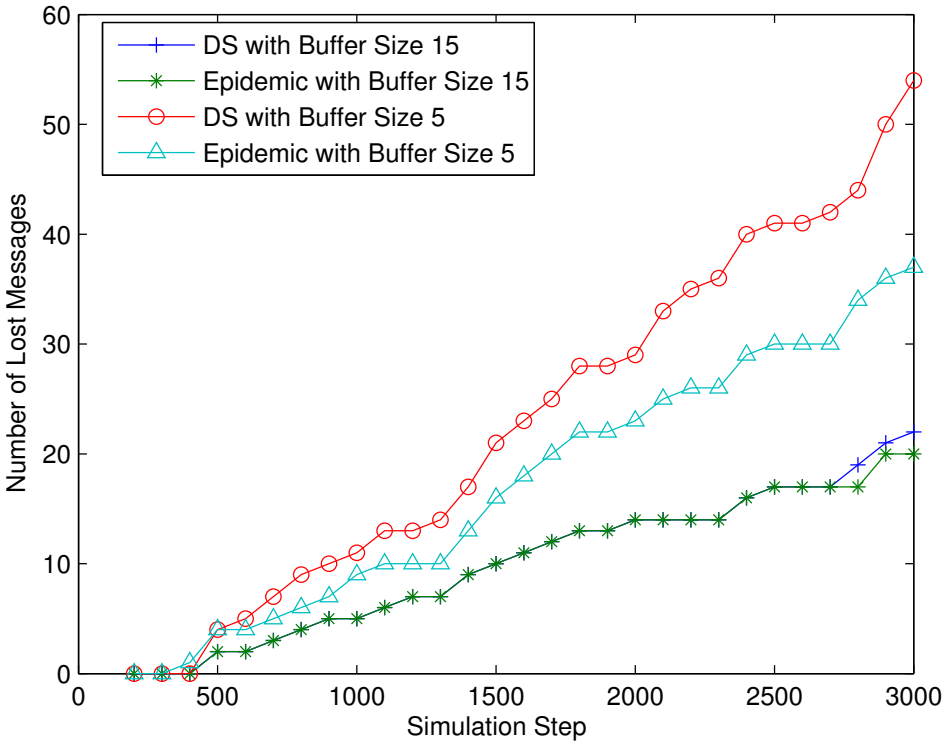

Figure 4.12: Comparison between the epidemic routing and dominating-set based routing with different buffer sizes in terms of the number of lost messages.

Figure 4.13 shows that the total number of messages forwarded with a small buffer size decreases in comparison with the case of a larger buffer size, but not proportional to the decrease of the buffer size. That is because reducing the buffer size not only increases the number of undelivered messages (as expected), but also the number of forwarded messages due to a n increased number of retransmissions of dropped messages because of the buffer space limitation. The

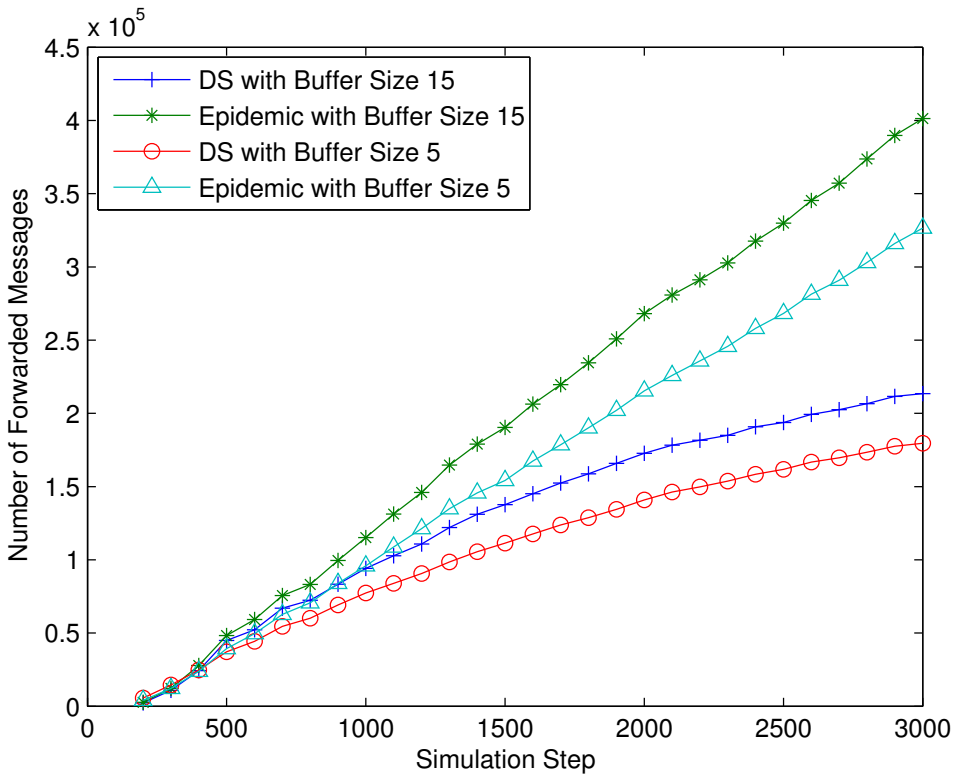

Figure 4.13: Comparison between the epidemic routing and dominating-set based routing with different buffer sizes in terms of the number of exchanged messages.

performance of both routing schemes degrade when the buffer size is reduced, but the dominating-set based routing still outperforms the epidemic routing in terms of the number of exchanged messages.

4.7 Summary

In this chapter, we consider routing over the super nodes system. We concentrate on routing over MANETs as a part of the super nodes system. We

introduce the concept of virtual network topology to adequately model a DTN based network with intermittent links. Constructing this topology requires an estimate of the probability of future contacts between nodes in the network. We propose to estimate the contact probability for nodes in MANETs based on the duration of previous contacts. We then propose a new routing technique based on calculating a connected dominating set of the constructed virtual network topology. Simulation results demonstrate that the newly proposed routing scheme outperforms the epidemic routing in terms of resources utilization, and that the estimation of the probability of future contacts between two nodes based on previous contact durations yields better routing performance than the estimation based on the number of previous contacts.

Chapter 5

Improving Routing Performance: Node Mobility Analysis

Dominating-set based routing for DTNs, introduced in Chapter 4, is based on the concept of virtual network topology. Unlike regular network topology where graph links represent physical connections among nodes, the virtual network topology defines a link between two mobile nodes as the probability of future contacts (*i.e.*, meetings) between the two nodes within the network. The routing technique is based on finding a connected dominating-set for the virtual network topology graph. The more accurate the virtual graph, the better the performance of the routing technique. The accuracy of the virtual network topology is mainly based on how accurate the probability of a contact between each pair of nodes can be estimated. In this chapter, we investigate how to exploit node mobility model to better estimate the probability of a contact between nodes.

Our contributions [1, 2] are four-fold: (i) we derive a node inter-meeting time distribution based on the proposed node mobility model and demonstrate the

accuracy of the distribution by a simulation study; (ii) we investigate how the proposed estimation of the contact probability can improve the performance of the dominating-set based routing scheme; (iii) we study how to relax the constraints of selecting the dominating-set members in order to achieve better resource utilization with acceptable performance by reducing the selected dominating set size; and (iv) we propose an alternative routing scheme based on selecting a random set and investigate how efficient the scheme is compared with the dominating set routing technique.

5.1 Estimation of the Contact Probability

As in real life, users usually have some patterns in their movements, we consider a Markov chain based user mobility model presented in Section 4.1.1. Similar models are also adapted in subsequent work by other researchers, such as in [91]. In this mobility model, the geographical service area of the MANET is partitioned to m partitions. A node-to-node direct communication takes place among nodes within the same partition. Node future location is independent of its past location, given its current location. The residence time of a node in a partition in each visit is an exponential random variable with parameter λ. For simplicity, we assume this parameter is the same for all the nodes and network partitions. Denote the location state of a mobile node by its current partition. Then, the user mobility model can be characterized by a one-dimensional continuous-time Markov chain where the node movement is described by the transition matrix $\mathbb{M}$, given by Equation (4.1).

Our goal is to analyze the node mobility model to get an accurate estimate for the probability of contact. We focus on the inter-meeting time between two nodes. Define inter-meeting time between a pair of nodes as the duration from

the instant that the two nodes move out of each other's transmission range to the instant that the two nodes move within each other's transmission range the next time. Define node inter-arrival time for a partition as the duration from the instant that the node departs from the partition to the instant that the node arrives at the partition the next time.

In the following, we first study the distribution of the node inter-arrival time for a partition, and then the distribution of the inter-meeting time.

Theorem 5.1. *The inter-arrival time of a node, A, to a partition, i, is an exponential random variable with mean* $\frac{1}{\lambda\pi_{A_i}}$*, where* π_{A_i} *is the limiting probability that node A resides in partition i.*

Proof. The continuous-time Markov chain for node A is irreducible. Hence, the limiting probabilities exist, satisfying the following equations:

$$\pi_{A_i} = \sum_{j=1}^{m} P_{L_{j,i}} \pi_{A_j} \ , \qquad i = 1, 2, \ldots, m \tag{5.1}$$

$$\sum_{i} \pi_{A_i} = 1. \tag{5.2}$$

The probability π_{A_i} is the fraction of time that node A resides in partition i. Define $N(t)$ as the number of all visited partitions by time t for node A. Then $N(t)$ is a Poisson process with mean λt (see *Appendix* A). Define $N_i(t)$ as the number of visits of node A to partition i by time t. Then $N_i(t)$ is a Poisson process with parameter $\lambda\pi_{A_i}t$. As a result, the inter-arrival time of node A to partition i is exponential with parameter $\lambda\pi_{A_i}$, i.e., with mean $\frac{1}{\lambda\pi_{A_i}}$.

□

Theorem 5.2. *The inter-meeting time between a node, A, and another node, B, is an exponential random variable with mean* $\frac{1}{\sum_{i=1}^{m} 2\lambda\pi_{A_i}\pi_{B_i}}$.

Proof. Nodes A and B meeting at partition i can occur in two scenarios: (i) Node A moves to partition i while node B already resides in partition i; and (ii) node B moves to partition i while node A already resides in partition i. Consider scenario (i), the number of meetings between the two nodes at partition i is the fraction of node A arrivals to partition i while node B is residing there. From *Theorem* 5.1 and noting that node B resides in partition i with probability π_{B_i}, the number of meetings between node A and node B at partition i when node A makes the movement is a Poisson process with mean $\lambda\pi_{A_i}\pi_{B_i}t$. Hence, the inter-meeting time between node A and node B at partition i when node A makes the movement is an exponential random variable with parameter $\lambda\pi_{A_i}\pi_{B_i}$. Similarly, for scenario (ii), the inter-meeting time between node A and node B at partition i when node B makes the movement is an exponential random variable with parameter $\lambda\pi_{B_i}\pi_{A_i}$. As a result, the inter-meeting time between node A and node B at partition i is a random variable that is the minimum of the two independent exponential random variables, which follows an exponential distribution with parameter $(\lambda\pi_{A_i}\pi_{B_i} + \lambda\pi_{B_i}\pi_{A_i})$. Considering all network partitions, the inter-meeting time between node A and node B is a random variable that has a distribution of the minimum of the the two nodes inter-meeting times at all the network partitions, which is an exponential random variable with parameter $\sum_{i=1}^{m} 2\lambda\pi_{A_i}\pi_{B_i}$.

□

Consider two nodes, A and B. Let P_{AB}^{T} denote the probability that a contact occurs between A and B, given that both of them are connected to the network over a time duration T. The probability of a contact based on the inter-meeting time between the nodes is

$$P_{AB}^{T} = 1 - e^{-\sum_{i=1}^{m} 2\lambda \pi_{A_i} \pi_{B_i} T}. \tag{5.3}$$

In this chapter we analyze the proposed mobility model. Most previous research works in DTNs employed the random way mobility model which is found to be too simple to characterize real life user roaming over different wireless network coverage areas. Many research efforts have been devoted to this area [92, 93]. There is no general mobility model for DTNs, however many research works that used real user traces such as [94, 95] and/or different node mobility models such as [96] have reached conclusions, similar to our analysis, that the node inter-meeting time can be approximately described by an exponential distribution. Moreover, we assume independent node inter-meeting times, which is an assumption adapted in many research works in the field of DTN such as the work in [97]. Similarly, the research work that is based on the analysis of real user traces such as the work in [94, 95] has reached the same conclusions as those assuming independence inter-meeting times.

5.2 Updated Dominating-set Routing

To apply the mobility model analysis to the dominating-set routing scheme, we use the expected inter-meeting time as a measure of link existence, which provides an estimation of how frequently two nodes will meet in the future. As a result, we can establish a virtual network topology as an undirected graph $\hat{G} = (V, \hat{E})$, where V represents the set of mobile nodes currently connected to the network and $\hat{E}$ is the set containing the expected inter-meeting times between any two nodes. Algorithm 5.1 is a modified version of the dominating-set selection algorithm (Algorithm 4.1), where τ_{ij} is the inter-meeting time between node i and node j, and $NG(i)$ is the set of neighbours for node i.

Algorithm 5.1 Calculating a connected dominating-set (DS) based on node inter-meeting times

Data: $G = (V, \hat{E})$: Virtual network topology connected weighted graph;

V: set of nodes;

$\hat{E}$:set containing the expected inter-meeting times, τ_{ij}, between each node pair (i, j);

Result: DS : set represents the calculated dominating set;

1: Start with DS contains only the gateway node
2: **for all** node $i \in V$ *and* $i \notin DS$ *and* $\{NG(i) \cap DS\} \neq NG(i)$ **do**
3: get min $E[\tau_{ij}]$ where $j \in NG(i)$ *and* $NG(j) \backslash \{i\} \neq \phi$
4: **if** $j \notin DS$ **then**
5: add j to DS
6: **end if**
7: **end for**
8: Get connected components in DS by recursively connecting each node $i \in DS$ with node j *where* $j \in NG(i)$ *and* $j \in DS$
9: **if** step 8 results in more than one connected components **then**
10: Select 2 components and find shortest path with lowest sum of weights connecting them over the graph G
11: **for all** node i in the calculated path **do**
12: **if** $i \notin DS$ **then**
13: Add node i to DS
14: **end if**
15: **end for**
16: GOTO step 8
17: **end if**

5.3 Dominating-set Selection Constraints Relaxation

Increasing the dominating-set size (*i.e.*, number of nodes in the set) improves the probability of message delivery by reducing the number of lost (*i.e.*, undelivered) messages, at the cost of increasing the number of message forwarded. The extreme case is that the dominating-set includes all the nodes in the network, which corresponds to the epidemic routing. Selecting dominating-set members based on the greedy Algorithm 5.1 does not take into consideration the dominating-set size, as each node selects the node with minimum expected inter-meeting time. The computation of the minimum connected dominating set over a given graph is an NP-complete problem [98], so approximate techniques are necessary for practical calculations. There has been a number of approximate techniques to calculate a dominating set for a network [99]. However, for the problem under consideration, the edge weight must be taken into consideration in selecting the domination set. In the following, we study the problem of reducing the dominating-set size and propose an alternative dominating-set selection algorithm. The new algorithm improves the routing performance in terms of resource utilization, while achieving acceptable performance in terms of the number of lost messages.

Message delivery in the system under consideration takes place when a message carrier comes into contact with the message destination. For the dominating-set based routing, the message carrier can be either a dominating-set member or the message source itself (*i.e.*, in a case of direct contact). Assuming a sufficiently large node buffer space, message loss mainly occurs as a result of the message expiry before a contact between a carrier and the message desti-

nation takes place. In a regular network, the end-to-end message delay can be controlled by selecting the message route to enforce certain quality of service. On the other hand, in a delay tolerant network environment, it is so difficult to precisely estimate the end-to-end delay of delivering a message. Most research efforts in this problem try to give an estimation for the delay over a specific route. In [100], it is stated that finding all the routes from a given source to a given destination with exact calculation of the expected delay distribution is a NP-hard problem, where the delay calculation is based on the primary path that has the smallest expected delay. To apply this to the dominating-set selection problem, it requires to calculate the shortest path between nodes for every source and destination. Based on the calculated shortest paths for all the nodes, the optimal dominating-set can be selected. Considering network size and dynamics (*i.e.*, expected change in network memberships due to user roaming, disconnection, and power failure), the calculations will be very complicated and impractical.

As shown in Figure 5.1 where the dominating-set has N nodes, the message end-to-end delay, denoted by T_D, for a no-direct contact case under the dominating-set routing consists of three delay components: the delay τ_S for the message source to deliver the message to the dominating-set, the delay τ_{DS} for the message over the dominating-set, and the delay τ_D to deliver the message from the dominating-set to the destination node. The expected end-to-end delay can be expressed as

$$E[T_D] = E[\tau_S] + E[\tau_{DS}] + E[\tau_D]. \tag{5.4}$$

The delay over the dominating-set, τ_{DS}, can range from 0 in the case of two hop path delivery to $\sum_{i=1}^{N-1} \tau_{i,i+1}$. Note that $\tau_{i,j}$ is a random variable that represents the time for node i to meet node j. As we assume no control on node mobility,

the only way to reduce these delay components is by selecting more nodes in the dominating-set. However, that will increase the number of forwarded messages, which causes inefficient use of the system resources. Minimizing the size of the dominating set improves the system performance in terms of the number of forwarded messages, however it increases the number of lost messages as it increases the expected delivery time. As a tradeoff solution, we propose to change the dominating-set selection criterion from selecting the nodes most likely to meet with each node in the network to selecting a minimum set of nodes so that every node in the network is expected to meet with a member of the set within a time interval less than certain threshold value θ_t on average.

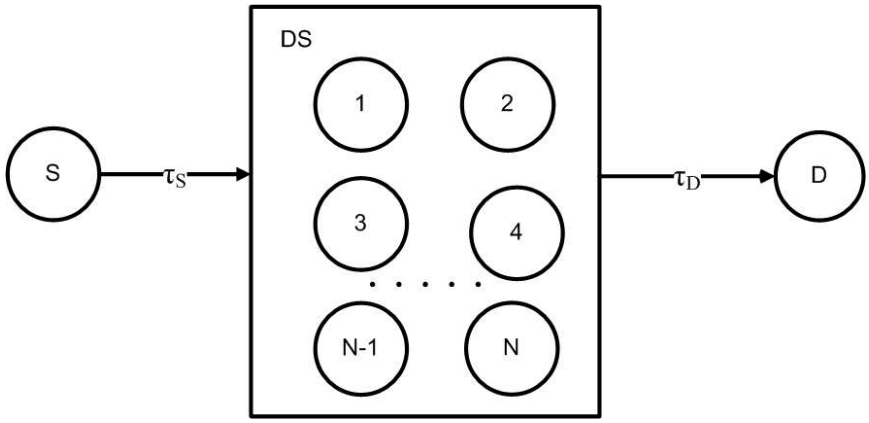

Figure 5.1: End-to-end message delivery under dominating-set based routing.

Based on *Theorem* 5.2, the inter-meeting time between a node, A, and any other node, X, that is a member of the dominating-set is an exponential random variable with parameter λ_{AX}, given by

$$\lambda_{AX} = \sum_{i=1}^{m} 2\lambda \pi_{A_i} \pi_{X_i} \tag{5.5}$$

for the network coverage with m partitions.

As a result, the inter-meeting time between node A and the dominating-set (excluding A if A is a DS member) is the minimum of the inter-meeting times between A and the DS members, which is an exponential random variable with parameter λ_A, where

$$\lambda_A = \sum_{X \in DS \setminus \{A\}} \lambda_{AX}. \tag{5.6}$$

Using Equation (5.4), reducing the expected end-to-end delay can be achieved by reducing the individual delay components, thus by reducing the expected inter-meeting time between an individual node and the dominating-set. The newly proposed algorithm, given in Algorithm 5.2, selects dominating-set members by including a small set of nodes so that every node in the network has an expected inter-meeting time with the set less than θ_t. The algorithm starts with a set, DS, containing only the gateway node. A node, A, will be added to DS only if there exists a node B where $E[\tau_B] \geq \theta_t$ and $E[\tau_{AB}] = min(E[\tau_{XB}]), \quad \forall X \in NG(B)$, where τ_{AB} is the inter-meeting time between A and B, τ_B is the inter-meeting time between node B and DS, and $NG(B)$ is the set of neighbours for node B. As a result, increasing θ_t is expected to reduce the DS size.

Unlike Algorithm 4.1 and Algorithm 5.1, processing a node, A, will result in adding its most probable node to meet, B, to the DS, only if the expected time of node A to meet with a dominating set member does not satisfy the required criterion θ_t. For sufficiently large θ_t, the dominating set may contain only the gateway, which is similar to the case of direct transmissions. As a result, the newly proposed algorithm, Algorithm 5.2, is expected to improve the system performance in terms of the number of forwarded messages as it can result in a reduced DS, as discussed next.

Algorithm 5.2 Calculating a connected dominating-set (DS) based on constraints relaxation

Data: $G = (V, \hat{E})$: Virtual network topology connected weighted graph;

V: set of nodes;

$\hat{E}$: set containing the expected inter-meeting times, τ_{ij}, between each node pair(i, j);

Result: DS : set represents the calculated dominating set;

1: Start with DS contains only the gateway node
2: **for all** node $i \in V$ **do**
3: $\lambda_i = \sum_{X \in DS \setminus \{i\}} \lambda_{iX}$
4: $\tau_i = \frac{1}{\lambda_i}$
5: **if** $\tau_i < \theta_t$ **then**
6: Skip next steps and get next $i \in V$
7: **end if**
8: get min $E[\tau_{ij}]$ where $j \in NG(i)$
9: **if** $j \notin DS$ **then**
10: add j to DS
11: **end if**
12: **end for**

5.4 A Network Example

In this section, we consider an example based on a typical simulation experiment to show how the different algorithms will process a typical scenario. The network consists of 7 nodes and the gateway S. This network is a fully connected graph. For presentation clarity, the topology is represented in a table format, given in Table 5.1. This table presents the probability of contact for each pair of nodes in the network based on the processed statistics of the contact duration among the nodes. For example, node A has a probability of 49% to contact node B, when both are connected to the network, and a probability of 86% to contact the gateway S. It is important to note that contacts between any pair of nodes are disjoint events.

Table 5.1: Probability of contacts based on previous contact duration (percentage).

	Node ID							
	S	A	B	C	D	E	F	G
S	–	86	55	10	75	81	10	41
A	86	–	49	49	57	58	49	43
B	55	49	–	71	56	62	33	38
C	10	49	71	–	49	78	71	84
D	75	57	56	49	–	35	80	25
E	81	58	62	78	35	–	27	91
F	10	49	33	71	80	27	–	37
G	41	43	38	84	25	91	37	–

Applying Algorithm 4.1 over the virtual network topology presented in Table 5.1, the algorithm starts with a set, DS, that contains only the gateway S. Processing each node in an ascending order of node ID, the most probable node to meet node A is S which is already in DS. For node B, as the most probable

node to meet is node C, node C is added to DS. Node C is not processed as it is already in DS. For node D, node F is the most probable node to meet and it is added to DS. For node E, the most probable node to meet is node G, so node G is added to DS. Nodes E and G are skipped from processing as they are members of the selected set. At the end of the first phase, the dominating set is $DS = \{S, C, F, G\}$. The second phase that guarantees the connectivity of the set is not necessary in this scenario as the graph is fully connected.

To apply Algorithm 5.1, it is required to calculate the expected inter-meeting time between each pair of nodes based on their mobility pattern, which is given in Table 5.2.

Table 5.2: Inter-meeting time (Simulation step).

	Node ID							
	S	A	B	C	D	E	F	G
S	–	41	31	180	35	28	91	60
A	41	–	52	49	53	40	60	54
B	31	52	–	46	50	50	60	46
C	180	49	46	–	42	46	46	41
D	35	53	50	42	–	40	33	48
E	28	40	50	46	40	–	50	47
F	91	60	60	46	33	50	–	52
G	60	54	46	41	48	47	52	–

Based on Table 5.2, Algorithm 5.1 starts with a set, DS, that contains only the gateway S. Processing each node in an ascending order of node ID, the resulting $DS = \{S, E, G, F\}$, which is a connected set.

It should be noticed that Algorithm 4.1 and Algorithm 5.1 result in different sets for the same problem as they process virtual network topology constructed based on different criteria, given in Table 5.1 and Table 5.2 respectively.

Reducing the size of the dominating set is the main design goal for Algorithm 5.2. This algorithm ensures that each node in the network has an expected inter-meeting time with the selected dominating set members less than a specific threshold value. If this cannot be achieved, the algorithm adds (to the selected set) the node with the least expected inter-meeting time (similar to Algorithm 5.1).

For the network scenario, $Message\ TTL = 90$ and $\theta_t = \frac{Message\ TTL}{2}$. Algorithm 5.2 starts with a set, DS, that contains only the gateway S. For node A , $\tau_A = 41$, so node A will not select any more nodes to be in DS as $\tau_A < \theta_t$. For node B, $\tau_B = 31$, similar to node A case, processing node B will not add any nodes to DS. For node C, $\tau_C = 180$, so node C selects the node with the least expected inter-meeting time which is node G to be added to DS. For node D, where $DS = \{S, G\}$, $\tau_D = \frac{1}{\frac{1}{35}+\frac{1}{48}} = 23.23$, so node D will not select any more nodes to be in DS. For node E, $\tau_E = \frac{1}{\frac{1}{28}+\frac{1}{47}} = 17.54$, so node E will not select any more nodes to be in DS. For node F, $\tau_F = \frac{1}{\frac{1}{91}+\frac{1}{52}} = 33.09$, so node F will not select any more nodes to be in DS. Node G is processed for the set $DS \backslash \{G\}$ as G is a dominating set member. As $\tau_G = 44 < \theta_t$, no more nodes are added to the set. The selected dominating set will be $DS = \{S, G\}$.

Given a reasonable value of θ_t, the new algorithm should result in a reduced size dominating set. All the algorithms for determining a dominating set for a virtual network topology are based on the idea of selecting a set of carrier nodes that cover the whole graph. It is expected that with a smaller dominating set size, the routing performance will be improved as the number of forwarded messages will decrease. With a fully connected network topology, selecting a random set of nodes can be regarded as an alternative approach. The main advantages are that there is no need to collect network statistics and to perform

dominating set selection computation as with the discussed algorithms. This is expected to reduce the computation overhead related to constructing and processing the virtual topology and to reduce the network overhead related to collecting the network statistics from the different nodes. This alternative approach is evaluated through our experiments in Section 5.5.

5.5 Performance Evaluation

We extend the simulation experiments introduced in Section 4.6 as follows. This section presents analytical results in comparison with simulation results for the inter-arrival time and the inter-meeting time. Moreover, we evaluate the performance of the dominating-set based routing scheme based on the user mobility model analysis and the newly proposed algorithm that relaxes the selection constraints. The performance is compared with that of epidemic routing and of the dominating-set based routing scheme using Algorithm 4.1. The performance is measured in terms of (i) the numbers of delivered and lost messages to indicate how reliable each technique is in delivering messages, and (ii) the number of forwarded messages over the network to demonstrate how efficiently each technique uses the available resources (i.e., radio bandwidth and node buffer space).

In the simulation, the number of partitions of the MANET coverage area varies in range of $10 - 50$. Each simulation proceeds in discrete time steps. Mobile nodes move with mobility trajectories independent of each other. For each simulation run, the movement matrix $\mathbb{M}$ of each node is generated at random and stays fixed till the end of the simulation. Initially, the node locations are uniformly distributed over the service area. As the simulation time increases, each node moves randomly according to its transition matrix. The node residence time at each partition is an exponential random variable with an average

of 10 simulation steps. At the end of the residence time, the node moves to a new partition based on its mobility matrix. Messages are generated in the network based on a Poisson process with mean rate of $\frac{9}{10}$ messages per simulation time step, with a constant message size. The source and the destination for each message are selected at random. The message time to live is constant with a value of 50 simulation steps. Each mobile node has a buffer space of 15 messages. The gateway has a buffer space of 2000 messages. A buffer overflow occurs when a node buffer is full and a new message is received. When a buffer overflow occurs, the oldest message in the buffer is discarded. Message exchanges occur among nodes residing in the same partition. We assume that the traveling time between partitions is small and can be neglected as compared to the partition residence time. At each time step, the node detects its neighbor nodes and exchanges the buffered messages with them (the messages they do not already have) based on the used routing technique. For each experiment, a communication scenario (i.e., set of messages, user connections, user disconnections, user movements) is set up randomly and run for each routing technique. For simplicity of simulation, we assume that each node can access the medium reliably.

Our first experiment is to validate the distribution of the inter-arrival time by simulation. In this experiment, we record node inter-arrival times for different partitions in the network. Based on the simulation recorded data, the mean and the 95% confidence interval are calculated and compared with the theoretical mean value obtained by applying Theorem 5.1. It is observed that the theoretical mean gives a very good approximation to the simulated data mean, which lies within the calculated 95% confidence interval of the simulation data. Table 5.3 shows a sample of the simulation results for a node moving over a network consisting of 10 partitions.

Table 5.3: Statistics of the node inter-arrival time.

Partition	**Simulation**		**Analysis**
ID	**Mean**	**Confidence interval**	**Mean**
1	62.59	54.10 – 71.08	66.25
3	80.54	65.69 – 95.39	80.63
4	51.83	44.01 – 59.65	56.36
5	59.57	51.11 – 68.03	57.04
8	90.64	73.60 – 107.68	90.59
9	127.44	99.00 – 155.88	120.04
10	126.58	104.35 – 148.80	122.12

Our next experiment is to validate the distribution of the node inter-meeting times by simulation. In this experiment, we track node-to-node inter-meeting times for each pair of nodes in the network. Table 5.4 shows the simulation results for tracking 4 nodes over a network of 10 partitions and compares them with the results calculated based on Theorem 5.2. It is observed that the simulation and analytical results match well.

Table 5.4: Statistics of the node inter-meeting time.

Node	**Simulation**		**Analysis**
pair	**Mean**	**Confidence interval**	**Mean**
$1, 2$	59.00	49.82 – 68.18	54.83
$1, 3$	52.97	45.38 – 60.55	50.24
$1, 4$	51.87	44.60 – 59.14	49.53
$2, 3$	48.83	41.80 – 55.87	44.77
$2, 4$	78.63	62.67 – 94.59	79.92
$3, 4$	61.82	50.89 – 72.75	62.70

In the following, we study the performance of the dominating-set based routing scheme using the node inter-meeting time as an indication of node-to-

node future contact frequency. The results are obtained by simulating a network with 20 partitions and 70 nodes.

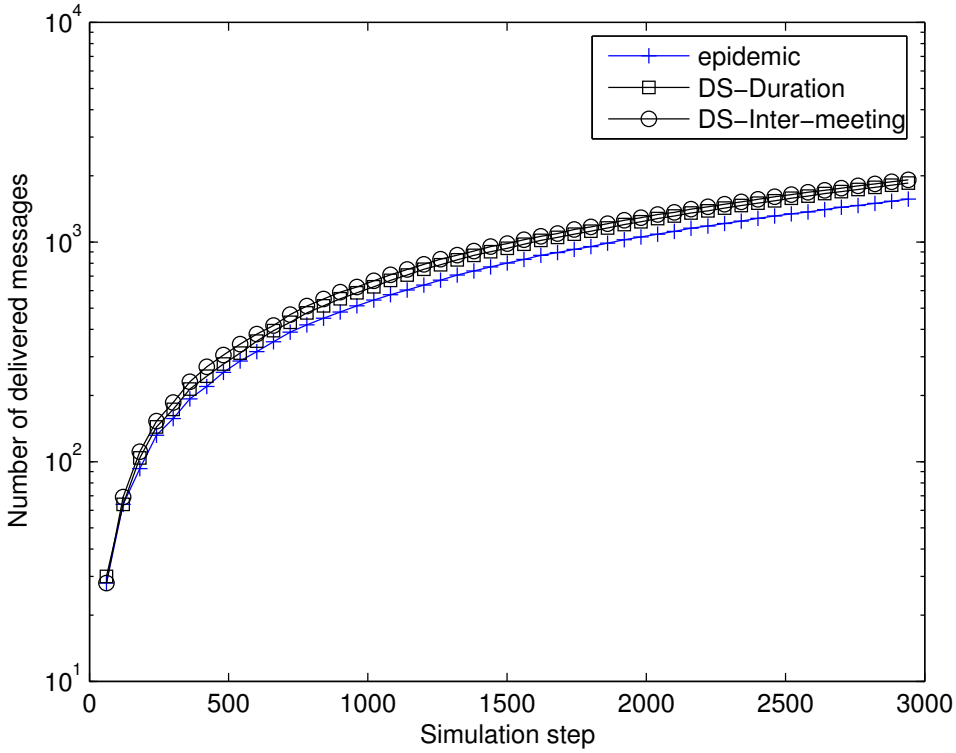

Figure 5.2: Number of delivered messages under different routing schemes.

Figure 5.2 shows a performance comparison in terms of the number of delivered messages between the epidemic routing scheme and the dominating-set based routing scheme using both criteria of (i) the inter-meeting time and (ii) the time based estimate of the probability of future contacts according to Equation (4.2). The dominating-set routing technique based on node inter-meeting times is found to slightly outperforms the other two schemes. This is demonstrated more clearly in Figure 5.3, which shows a comparison among the three schemes in terms of the number of undelivered (lost) messages. With the node

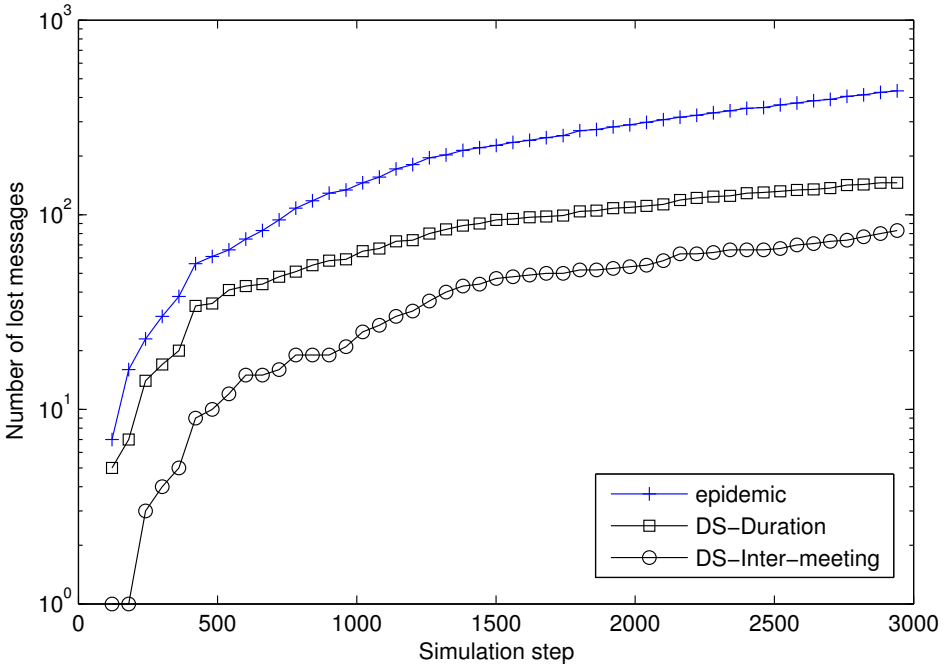

Figure 5.3: Number of lost messages under different routing schemes.

limited buffer space and an increasing number of exchanged messages, some messages are lost due to buffer overflow. Using the node inter-meeting times as a selection criterion ensures that message carriers are more likely to be in contact with the message destination in a shorter duration.

Figure 5.4 shows a performance comparison in terms of the number of forwarded messages as a measure for the network resource utilization. It is clear that the dominating-set routing scheme based on the node inter-meeting times gives the best performance among the three schemes. This is mainly due to the accurate selection of the dominating set members that results in a reduced number of forwarded messages required to achieve message delivery.

On the other hand, experimenting with an increased node buffer size shows that the three schemes give comparable results in terms of the number of delivered messages and the number of lost messages (due to a decrease in buffer overflow). However, the dominating-set routing scheme based on the node inter-meeting times consistently gives the best performance in terms of the number of forwarded messages. Considering the inevitability of having a limited node buffer space, it is clear that a more intelligent buffer management scheme can improve the performance of the routing schemes, which is interesting topic for further research.

We extend our experiments by implementing the newly proposed algorithm (i.e., Algorithm 5.2) for selecting dominating-set members based on the criterion of limiting the expected node inter-meeting with the dominating-set to a threshold value θ_t. Figure 5.5 and Figure 5.6 show the results with different values of θ_t,
where $\theta_1 = \frac{Message\ TTL}{2}$ and $\theta_2 = \frac{Message\ TTL}{5}$.

Figure 5.5 shows how the new algorithm improves the performance in terms of the number of forwarded messages as compared to the case of using Algorithm

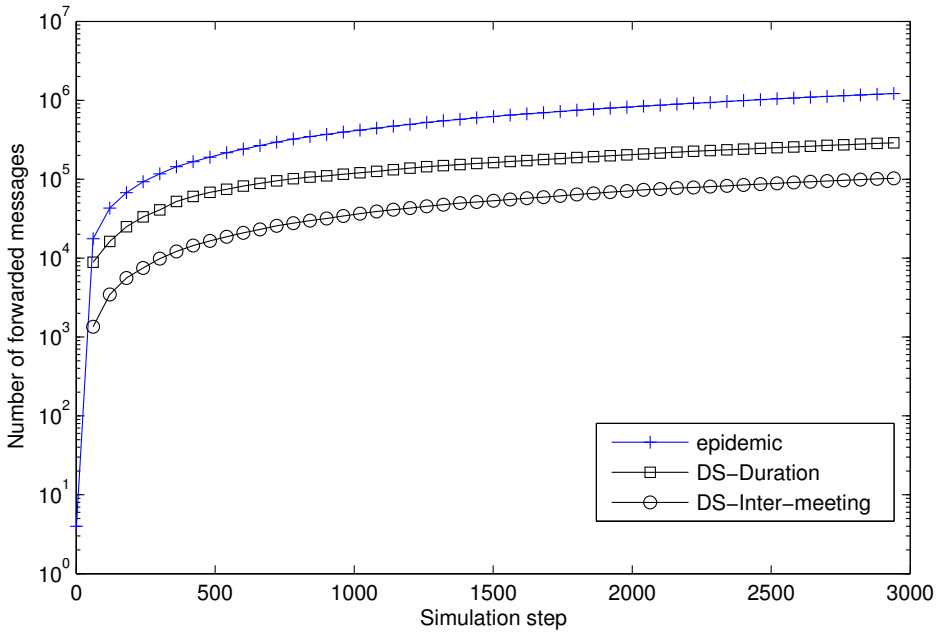

Figure 5.4: Number of forwarded messages under different routing schemes.

5.1 and the case of epidemic routing. Increasing the threshold value gives better results in terms of forwarded messages, but decrease the performance in terms of the number of lost messages as shown in Figure 5.6. It is noticed that Algorithm 5.2 outperforms Algorithm 5.1 in terms of the number of forwarded messages with acceptable performance in terms of the number of lost messages. This is mainly because, under the new criterion, the dominating set size is reduced.

As Figure 5.6 shows, the number of the lost message under Algorithm 5.2 is larger than that under Algorithm 5.1. This is because increasing message holding time at a carrier node (i.e., DS member) increases the probability that the message being discarded before being delivered due to a buffer overflow. With a larger node buffer space, it is noted that both Algorithms 5.1 and 5.2 give comparable results. This is because message loss in this case is mainly due

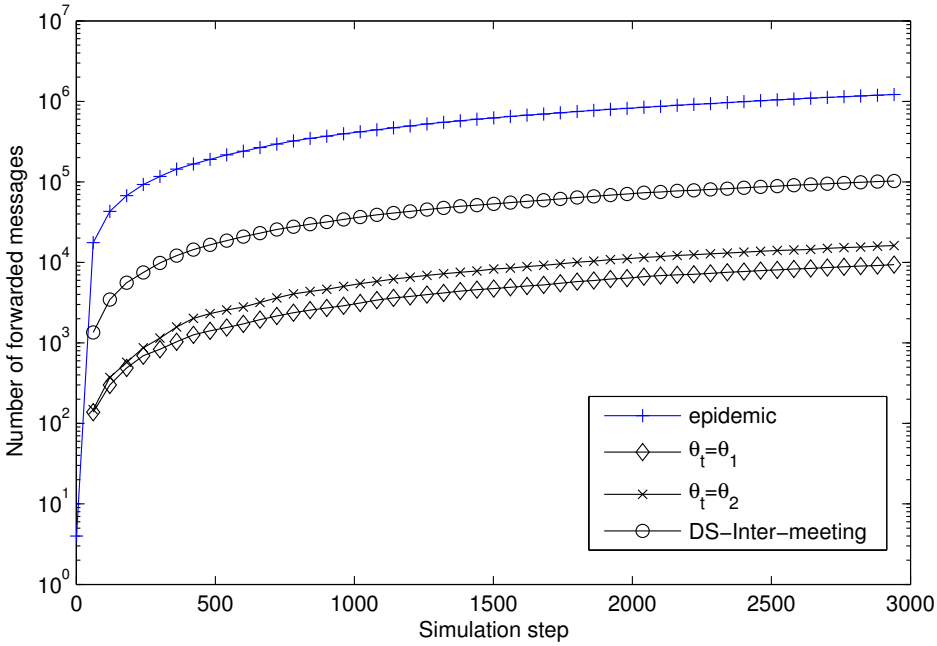

Figure 5.5: Number of forwarded messages under different routing schemes and different threshold values.

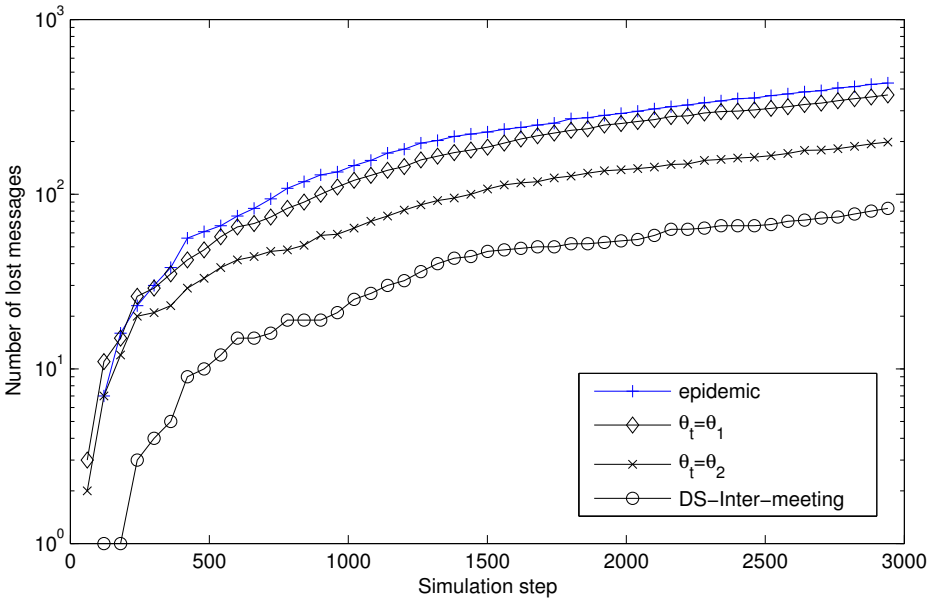

Figure 5.6: Number of lost messages under different routing schemes and different threshold values.

to the message expiry, but less likely due to buffer overflow. It is also noted that, regardless of the buffer space, Algorithm 5.2 outperforms Algorithm 5.1 in terms of the number of forwarded messages. The threshold value θ_t plays an important role in the performance based on Algorithm 5.2. How to determine a proper θ_t value, for a given network scenario, requires further investigation.

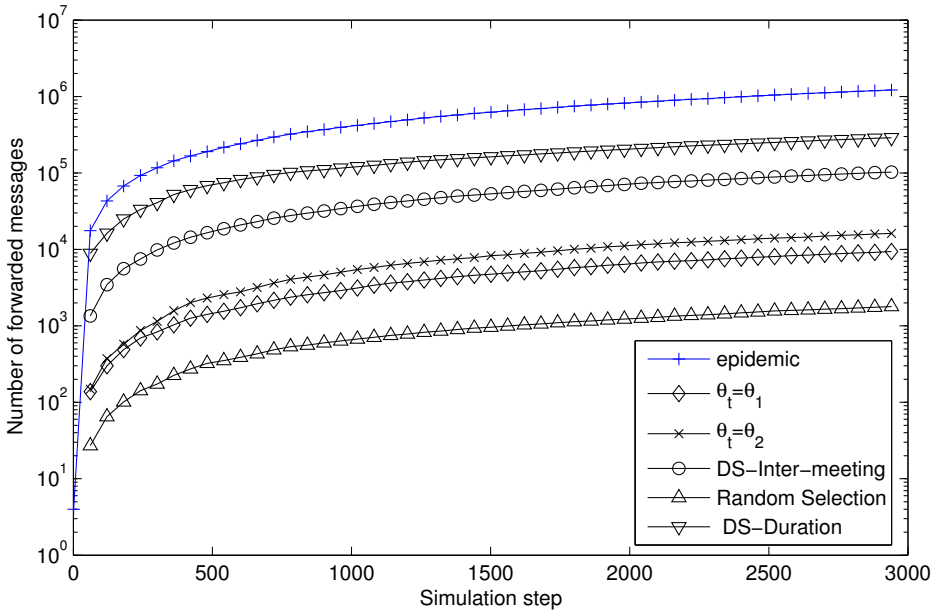

Figure 5.7: The random selection technique performance compared to the other techniques in terms of the number of forwarded messages.

Our last experiments investigate the performance of the random set selection technique (discussed in Section 5.4), in comparison with the other techniques, as illustrated in Figures 5.7- 5.8. The DS size is set to the smallest DS size from the discussed algorithms, but the DS members are selected randomly. Figure 5.8 shows that the random selection technique degrades the performance significantly even when compared with the worst performance of the other techniques. In other words, reducing DS size alone does not improve the performance unless

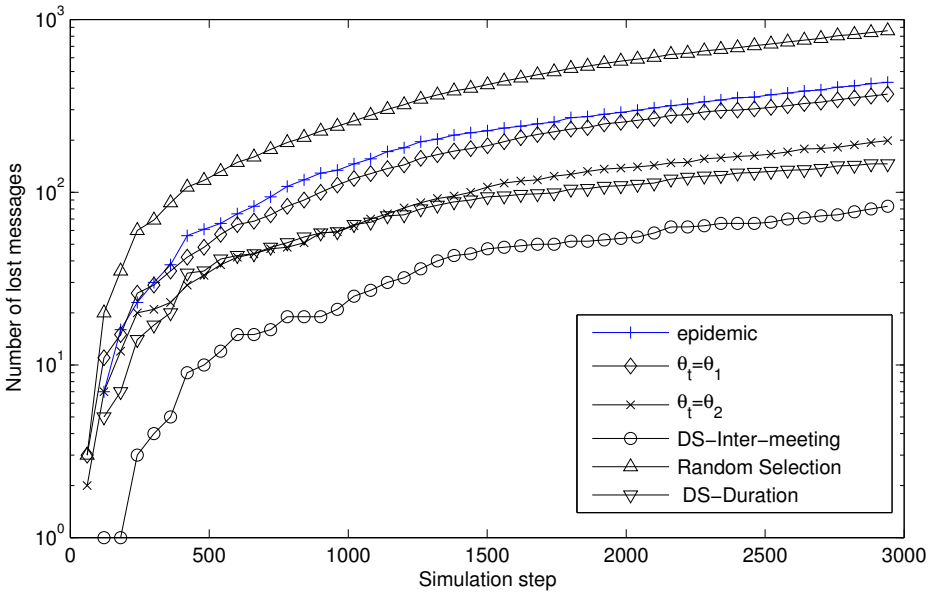

Figure 5.8: The random selection technique performance compared to the other techniques in terms of the number of lost messages.

an accurate selection methodology for the DS members is employed to guarantee proper contacts between the set members and the other nodes. The number of lost messages increases due to the lack of contacts between the set members and the other nodes, which causes messages to expire before being delivered. This decrease in contacts also leads to the smallest number of forwarded messages (as shown in Figure 5.8) as compared to the other techniques. Reducing the number of forwarded messages in this case cannot be regarded as a performance improvement because of the significant degradation in the performance in terms of the number of lost messages.

5.6 Summary

In this chapter, we consider the dominating-set based routing for a DTN based MANET within the super nodes system. We analyze the node mobility to better estimate node-to-node future contact statistics for improving message delivery. The node inter-meeting time distribution is derived based on a Markovian node mobility model, which is validated by a simulation study. The mean node inter-meeting time is used in the dominating-set routing scheme. Computer simulation results demonstrate that the dominating-set routing scheme based on the mean node inter-meeting time outperforms epidemic routing and dominating-set routing based on previous contact duration, in terms of both message delivery rate and resource utilization. Moreover, we propose a new algorithm for selecting the dominating-set based on the distribution of node inter-meeting time, which results in a smaller dominating-set size. The newly proposed algorithm chooses a set of nodes so that every node in the network should have an expected inter-meeting time with the set members under a certain threshold value. The computer simulation results show the effectiveness

of the proposed new algorithm. Using the proposed technique of choosing the dominating set randomly is shown to be inefficient. It is shown that not only reducing the dominating set size improves the performance, but the accuracy of choosing the dominating set members is a main factor for routing performance.

Chapter 6

Message Security and Network Access

6.1 Problem Overview

The nature of the DTN environment introduces new security constraints and challenges [101, 102]. Long delays combined with the lack of continuous communications with a network server introduce new challenges in information security for mobile nodes in a DTN environment. Many new challenges have been addressed for this environment such as how to stimulate positive cooperation among nodes. Nodes cooperation is very essential in this environment for successful communications [85]. Many studies have been addressing this issue using reputation based schemes [103] or credit-based schemes [104–106]. Among challenges in a DTN due to long delays and frequent disconnections, one major open issue is how to limit unwanted (*i.e.*, unauthorized) traffic within a network. The problem of preventing unauthorized traffic in regular networks is handled analogues to the problem of authentication, authorization and account-

ing (AAA). Authenticating a user and assigning access privileges in traditional networks are performed by a special network node such as an access point in a wireless local area network (WLAN), a base station in a cellular network, or a trusted server in general. In DTN, long delays and frequent disconnections make a continuous contact with such trusted server impossible. As a result, a new scheme is required to cope with the new constraints.

In DTN, an end-to-end route between the message source and the destination consists of a sequence of intermediate nodes, in addition to the end nodes. These intermediate nodes can either play a special role in the network such as message mules [44, 56] or be regular nodes [6]. The process of message delivery requires message storing and forwarding by intermediate nodes, which consumes network resources in terms of node buffer space and radio spectrum bandwidth. As a result, identifying and limiting unauthorized messages will reduce the overhead imposed on the network. However, this requires the intermediate nodes to be able to authenticate each message and verify its original sender's eligibility to use the network before accepting the message. There is no general solution proposed for this problem within the DTN architecture [102]. Most of existing solutions are highly specialized to a specific network scenario. For example, the work in [107] assumes that each node knows all eligible nodes' public keys. When a message is received, the signature is verified against all known eligible public keys. This technique is difficult to scale for a large network with increased number of nodes. Related techniques have been introduced for a vehicular network, such as the HAB (huge anonymous keys based) protocol [108]. The HAB protocol is to secure vehicular networks where each node possesses a huge set of keys to sign messages. There are many techniques that use the same idea of asymmetric key cryptography with a pre-distributed set of keys at each node such as [109], [110] and [111]. A problem with all these techniques is the exten-

sive use of asymmetric key cryptography, which consumes a significant amount of resources in terms of node computing power. This problem is addressed for vehicular networks in [112], where the proposed solution uses symmetric key cryptography, when a connection is available with a road side unit (RSU), to reduce the overhead.

Using asymmetric key cryptography in the DTN environment for message authentication introduces computation overhead over intermediate nodes. Table 6.1 shows a comparison of the computational requirements for different asymmetric key cryptographic signing algorithms such as RSA and ECDSA. The results in the table are based on running the Crypto++ 5.6.0 [113] benchmark on Intel Core 2 1.83 GHz processor under Windows Vista in 32-bit mode. As shown in Table 6.1, the asymmetric key techniques introduces extra computation overhead, in terms of the required computations to perform the operation, compared with the computation required when using symmetric key techniques as shown in Table 6.2. The computation overhead is a critical factor in a DTN environment as the nodes are devices with limited battery power. Moreover, in terms of the security strength of the symmetric key techniques in comparison with asymmetric key techniques, Table 6.3 [116] shows a security strength comparison among suite B [117] different cryptography algorithms. The AES technique, even with small size key, can be comparable to ECDSA and RSA with much larger size keys. An intermediate node in DTN networks has to perform a verification operation for each received message to be accepted for storing in its buffer and for forwarding. As a result, we choose the RSA technique for our discussion as the RSA verification operation requires less computation overhead compared to the RSA signature operation. Moreover, using asymmetric key cryptography techniques for message authentication implies additional communication overhead. The communication overhead is introduced due to the need

to exchange the public key certificate of message sender with the message. The certificate size is in terms of hundreds of bytes if ECDSA is employed or in terms of kilobytes if RSA is employed. This transmission overhead is translated into additional transmission energy consumption overhead. As an example of this energy consumption, the work in [114] addresses that consumption for a Chipcon CC1000 radio used in Crossbow MICA2DOT motes to be 28.6 μJ to receive one byte and 59.2 μJ to transmit one byte. Many research efforts in DTNs, such as [115, 119], address this overhead by performing message batches processing.

It should be noted that we base our discussion on the Crypto++ benchmark as a reference. However, some existing hardware implementation can achieve much better performance for ECDSA. With the proper hardware implementation, ECDSA can be a much better choice than RSA, considering the smaller size for ECDSA keys compared to RSA keys as shown in Table 6.3. Our main solution addresses the problem of the overhead imposed by using asymmetric key techniques, by calculating the message authentication through symmetric key techniques such as AES.

Table 6.1: Asymmetric key based techniques benchmark [113].

Algorithm	Mega cycle per operation
2048-bit RSA signature	11.06
2048-bit RSA verification	0.29
ECDSA over GF(p) NIST P-256 signature	3.92
ECDSA over GF(p) NIST P-256 verification	6.56

Another major open issue in a DTN is how to secure end-to-end message exchanges. Unlike regular networks, it is difficult in a DTN environment to control message route. A malicious intermediate node that gets a copy of a message

Table 6.2: Symmetric key based techniques and cryptographic hash functions benchmark [113].

Algorithm	Cycle per byte
AES with 256-bit key	18.2
AES with 128-bit key	16.0
SHA-1	11.4
SHA-256	15.8
SHA-512	17.7

Table 6.3: Security strengths comparison for a subset of the NSA suite B cryptography algorithms [116].

Security strength	Symmetric key algorithms	IFC (RSA)	ECC (ECDSA, ECDH, ECMQV)	Digital signatures and hash-only applications
80	$2TDEA$	1024	$160 - 223$	$SHA - 1$
112	$3TDEA$	2048	$224 - 255$	$SHA - 224$
128	$AES - 128$	3072	$256 - 383$	$SHA - 256$
192	$AES - 192$	7680	$384 - 511$	$SHA - 384$
256	$AES - 256$	15360	512+	$SHA - 512$

can disclose and/or change the message contents. As a result, end-to-end message security (*i.e.*, message confidentiality and authenticity) is a necessity in a DTN. Secure end-to-end messages exchanges require mutual authentication between the communicating parties, i.e., the sender and receiver(s). In a large size network scenario, mutual authentication requires the communication with a trusted third party (*e.g.*, certificate authority). Traditional techniques for end-to-end security cannot be applied directly to a DTN environment due to the potential unavailability of a physical end-to-end path either between the message's sender and the receiver or between each of them and a trusted third party. Without available communications with a trusted third party, communicating parties are not able to perform mutual authentication in a timely manner to allow the communication. There are some adaptations of regular techniques to handle this problem within a DTN, such as the work in [118] which proposes to use Identity Based Cryptography (IBC) and to adapt the regular public key cryptography to achieve secure end-to-end message exchanges. The main idea is to minimize the required communication with a trusted third party to overcome the unavailiabity of a continuous connection with the trusted third party. However, most of the proposed techniques are based on asymmetric key cryptography. We propose a technique for achieving end-to-end secure message exchanges within the super node architecture, which employs symmetric key cryptography to reduce the computation overhead associated with asymmetric key cryptography. The main idea is to map the problem of node mutual authentication from the unreliable network domain (*i.e.*, between communicating nodes) to a reliable network domain (*i.e.*, between super nodes).

Our contributions [3, 4] can be summarized as five folds: i) Adopting traditional PKI based certificates for limiting unauthorized traffic within the super node system; ii) proposing the new idea of separating the problems of message

sender authentication and message authorization at an intermediate node; iii) introducing a new technique based on symmetric key cryptography, employing the concept of one-way key chain, and introducing the concept of key group to reduce the overhead induced by asymmetric key cryptography techniques; iv) evaluating the performance of the proposed techniques over different routing techniques; and v) introducing the idea of moving the problem of mutual authentication to super nodes in order to reduce overhead imposed on the communicating mobile nodes.

6.2 The System Model Assumptions

Preventing unauthorized traffic over the super nodes system implies preventing it over the access networks. However, within the super nodes system, some access networks already have a security infrastructure to prevent unauthorized nodes from using the networks such as cellular networks and secure WLANs. As a result, here we focus on wireless networks that do not have an infrastructure such as MANETs. The MANET model under consideration is similar to the model described in Section 4.1.

The role of granting network access to a mobile node should be assigned to a specific entity. This entity is determined based on the network under consideration. In our system model, the gateway grants network access to nodes currently connected through the network under its jurisdiction. The gateway is assumed to have no-knowledge about node private information such as passwords, current status, etc. In order to decide whether or not to grant access to a node, the gateway contacts the super node responsible for the node. The communication between the gateway and the super node is assumed to be reliable and secure over the Internet backbone. Each super node and the gateway have

a public-private key pair. Each node should know the public key of its super node. Each node has a public-private key pair and the public key is stored at its super node.

In developing a solution, the following assumptions are made:

1. Super nodes are trusted (similar to the trusted third party in regular networks);

2. Super nodes can be under different jurisdictions (*e.g.*, ownership), so that nodes' private information (*e.g.*, password, messages) may be not sharable among different super nodes;

3. Each super node has a public/private key pair, and the public key is known to all the other super nodes and to all the nodes under its jurisdiction;

4. Any node in the system knows its own super node's public key and does not have to know the public key of any other super node in the system;

5. Each node has a public/private key pair, and the public key is stored at its super node;

6. Super nodes and gateways can communicate with each other efficiently and securely over the Internet backbone;

7. A loose time synchronization can be achieved among nodes and super nodes, that all nodes and super nodes agree on the current time with an error tolerance less than message time to live (as will be discussed next).

In the rest of this chapter, we use the notations summarized in Table 6.4.

Table 6.4: The Notations Overview.

Notation	**Description**
ID_A	the public identifier of entity A
$\|$	message concatenation operation
S_A	the super node of node A
PK_A	the public key of node A
SK_A	the private key of node A
$Enc_K(\cdot)$	symmetric key encryption function with key K using AES
$Dec_K(\cdot)$	symmetric key decryption function with key K using AES
K_i	symmetric key with index i
$E_X(\cdot)$	asymmetric key encryption function with key X using RSA
$D_X(\cdot)$	asymmetric key decryption function with key X using RSA
$H(\cdot)$	one-way hash function such as SHA-1
$H^i(\cdot)$	applying hash function H for i times
$HMAC_K(\cdot)$	a keyed-hash message authentication code, which is generated with symmetric key K
KG_n	a key group of length n
PP	The public parameter for Private Key Generator (PKG)
$G(\cdot)$	Private key generating function for IBC technique

6.3 Preventing unauthorized network access

Within the MANET access network, any roaming node can send a message over the network. Regardless of the sender, the intermediate nodes will carry and forward this message to either its destination (if it is within the network) or the gateway (if the destination is in another network). The main goal of this work is to prevent the messages of unauthorized users to be carried over the network. However, unauthorized nodes can roam over the network and participate (if they want) in message forwarding of other authorized nodes, yet they cannot send their own messages. This assumption is based on the work introduced in [120] which argues that unauthorized nodes can help in delivering messages in the network as the unpredictable nature of a DTN reduces the effectiveness of tampering with message attacks to that of simple network failures. As a result, our goal is not to prevent unauthorized nodes from participating in message forwarding as data mules, but to prevent them from being able to send their own messages over the network.

One approach to solve the problem is to let intermediate nodes carry and forward a message regardless whether or not the sender is allowed to use the network resources (*i.e.*, to send the message over the network). As the message reaches the gateway, the gateway can check the message sender and discard the message. This solution does not prevent unauthorized traffic, because message discarding occurs at the gateway after an unauthorized message has already been carried over the network and sometimes it may be delivered without going through the gateway (*i.e.*, if the destination node is connected over the same network). However, this approach moves the message checking process to the gateway, which reduces message checking overhead imposed on the intermediate nodes. On the other hand, with an increased number of unauthorized messages,

the network performance degrades (as to be discussed in Section 6.5).

The two approaches proposed in the following depend mainly on attaching a message authentication code (MAC) block to each message. Using this block, any intermediate node can decide to carry the message or to discard it without the need to contact a third party. The difference between the two approaches is how to calculate the MAC block. The first approach is based on asymmetric key cryptography which is inefficient for the system model under consideration. This is mainly due to the computation overhead, as shown in Table 6.1, imposed over intermediate nodes. This overhead increases with increased number of forwarded messages, as the number of required message signature verifications increases. Moreover, attaching the public key certificate of the message source node to the message for verification increases the size of the transmitted/received data. This imposes energy overhead over an intermediate node as discussed in Section 6.1. As a result, the second approach is based on a new idea of redefining the problem to separate the message authorization from the message sender authentication. The second approach uses symmetric key cryptography to reduce the overhead encountered in the first approach.

6.3.1 PKI Certificate Based Scheme

Public key management is still an open problem for DTN security [102]. In our approach, public key certificate can be defined within the standard X.509 [121] public key certificates. However, X.509 implementations over a DTN have restrictions to adapt with the DTN constraints. The main concern we address is inefficiency of implementing Certificate Revocation List (CRL) checking due to the unavailability of a continuous connection between the certificate server and individual nodes over the network. Therefore, in our approach we define

certificate revocation based on the certificate expiration time only.

The gateway is the node that can decide which user is eligible to use the network resources, *i.e.*, it acts as a trusted third party. However, a continuous contact with the gateway from a mobile node is likely not possible to allow the intermediate nodes to verify message sender eligibility to use the resources. One possible solution is to let the gateway act as a certificate authority which issues a PKI certificate for each authorized user.

When a node, A, first connects to the network, it should contact its super node, S_A. This connection message must travel through the gateway to reach the super node:

$$\begin{aligned} ConnectMsg &\leftarrow ID_A \mid ID_{net} \mid TimeStamp \mid SIG_A, \\ SIG_A &\leftarrow E_{SK_A}(H(ID_A \mid ID_{net} \mid TimeStamp)). \end{aligned}$$

Based on the connection message, the super node can authenticate the user identity and inform the gateway whether or not this user should be granted access over the network and the period of granted access. As the super node knows the node public key, it constructs a permission message and sends it back to the gateway:

$$\begin{aligned} PermMsg &\leftarrow ID_A \mid ID_{net} \mid Duration \mid TimeStamp \mid PK_{gateway} \\ &\quad \mid PK_A \mid SIG_{S_A}, \\ SIG_{S_A} &\leftarrow E_{SK_{S_A}}(H(ID_A \mid ID_{net} \mid Duration \mid TimeStamp \\ &\quad \mid PK_{gateway} \mid PK_A)). \end{aligned}$$

As the node does not know the public key of the gateway, the super node includes the gateway public key in the permission message to authenticate the gateway. The gateway uses this message and issues a temporary certificate to

grant the node an access to the network:

$$Cert_A \leftarrow ID_A \mid ID_{net} \mid ExpTime \mid PK_{gateway} \mid PK_A \mid SIG_{gateway},$$
$$SIG_{gateway} \leftarrow E_{SK_{gateway}}(H(ID_A \mid ID_{net} \mid ExpTime \mid PK_{gateway} \mid PK_A)).$$

The node checks the authenticity of the certificate by checking the permission message. To send a message over the network, the node signs the message with its private key and sends the signed message with the certificate. Intermediate nodes can check the message authenticity by checking the certificate. This implies that each intermediate node performs two asymmetric cryptographic operations per carried message, one to check the message signature and the other to check the certificate itself. Based on the routing technique used, the intermediate node forwards the message with its certificate attached.

Limiting the certificate lifetime overcomes the problem of certificate revocation in order to revoke node access. Upon certificate expiration, the node can recontact the gateway to request more network access time. The problem with this approach is the overhead imposed by the required number of asymmetric key cryptographic operations. A message sender should sign the message in order to forward it. Each intermediate node receiving the message should verify the signature and the sender's certificate, which requires two verifications operations per forwarded message. An increased number of forwarded messages increases the computation overhead, as discussed in Section 6.1, over intermediate nodes which are expected to be power limited portable devices.

6.3.2 Symmetric Key Based Scheme

This main proposed technique uses symmetric key cryptography to reduce the number of required asymmetric key cryptograhic operations and hence the imposed overhead. The technique uses the concept of one-way key chain [122].

One-Way Key Chain

The one-way key chain [122] is a sequence of keys generated by consecutive applications of one-way hash function. Figure 6.1 shows the generation of one-

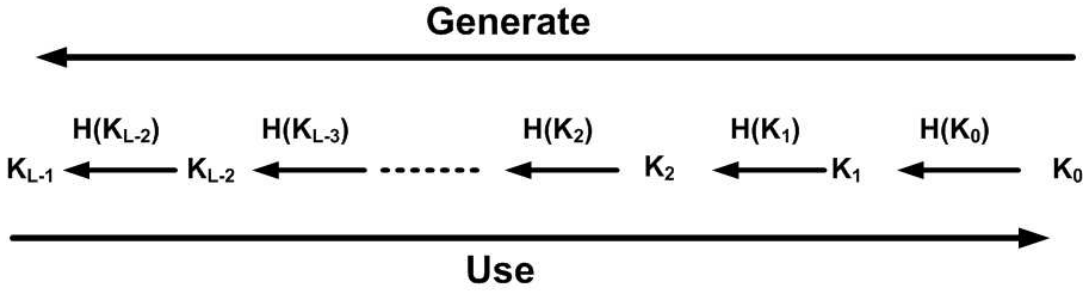

Figure 6.1: One-way key chain of length L.

way key chain with a seed key K_0, which is randomly chosen. The chain is generated by consecutive applications of one-way hash function $H(.)$ to the seed value (*i.e.*, key). Any key K_x can be used to reveal any subsequent key K_y, where $y \geq x$. By the one-way hash function definition, a key K_y cannot be used to obtain a key K_x where $x < y$ because this implies to reverse the one-way hash function. As a result, the direction of key usage, in the chain, is in the reverse direction of the key generation.

For example, for a key chain of length L with initial key K_0, the generation requires applying the hash function H for $L-1$ times; but the first key to use is K_{L-1}, the second key is K_{L-2}, and so on. To generate a key K_i, the hash function should be repeatedly applied for i times on the seed key:

$$H^i(K_0) \quad = \quad K_i, \qquad 0 < i < L.$$

A protocol, TESLA [122], is introduced to secure broadcast communication,

using a one-way key chain generated by the message sender. The sender computes a MAC block for each message based on the current key of the chain. As the message receiver cannot validate the message because the key is known only to the sender, it buffers the received messages until it receives the used key in a subsequent message. When the key is disclosed, it becomes useless for malicious nodes because its time frame is over. The main issue in TESLA is message delivery time synchronization between message sender and the receivers. TESLA cannot be used over a DTN because a message sender discloses the key to the receivers in subsequent messages. Long delays in a DTN will cause a very long delay between message reception and message approval. Quick disclosing of the key may speed up message approval, but it will cause delayed messages to be discarded. As a result, TESLA cannot be applied in a DTN where message delivery time cannot be controlled.

The proposed scheme

The introduced idea is based on the fact that the asymmetric key cryptography based technique not only proves the message legitimately, but also authenticates the sender identity which is not required in the problem under consideration. The authentication of the sender identity should be a problem of the message destination (not intermediate nodes), which is part of the process of establishing end-to-end security. Intermediate nodes need only to ensure that any received message is authorized to be carried over the network, but not to prove the identity of its sender.

With a symmetric key to compute a message signature using a key hashing algorithm, only authorized nodes should know the key that will be regularly updated by the network gateway. The network access time assigned to a node

varies depending on the node, similar to the certificate lifetime. The gateway can generate a set of keys, and each key is to be used within a time frame in the network. Nodes check each received message against the key used when the message are issued based on the message time stamp. Due to potential long delays in message delivery, existing messages may belong to different time frames and consequently different keys. This requires that a new node should receive not only the keys that cover its network access period but also old keys to participate in message forwarding. This is solved by employing the concept of one-way key chain.

The network gateway generates a key chain to be used over a long time period. The gateway splits the time period into equal durations (frames), and each key in the chain is used for a specified duration. Based on how long a node is permitted to access the network, a subset of the chain (*key group*) is shared with the node. To send a message, the sender node generates a MAC block using a key based on the message time stamp. Intermediate nodes check the MAC block against the shared key chain to check if the message is legitimate to be carried or not.

As shown in Figure 6.2, when a node, A, connects to the mobile ad-hoc network supervised by gateway, G, it sends a connection message to its super node. When the super node receives the message, it sends a permission message to the gateway. The gateway grants network access to this node for a specific time period by sending a key group that covers this period. For example, if the key lifetime is t_{key}, and the gateway wants to grant an access period of $5t_{key}$, then the gateway should send the current key and the next 4 keys to he node. We call the keys *key group* (KG). If the current key is K_x, the key group of

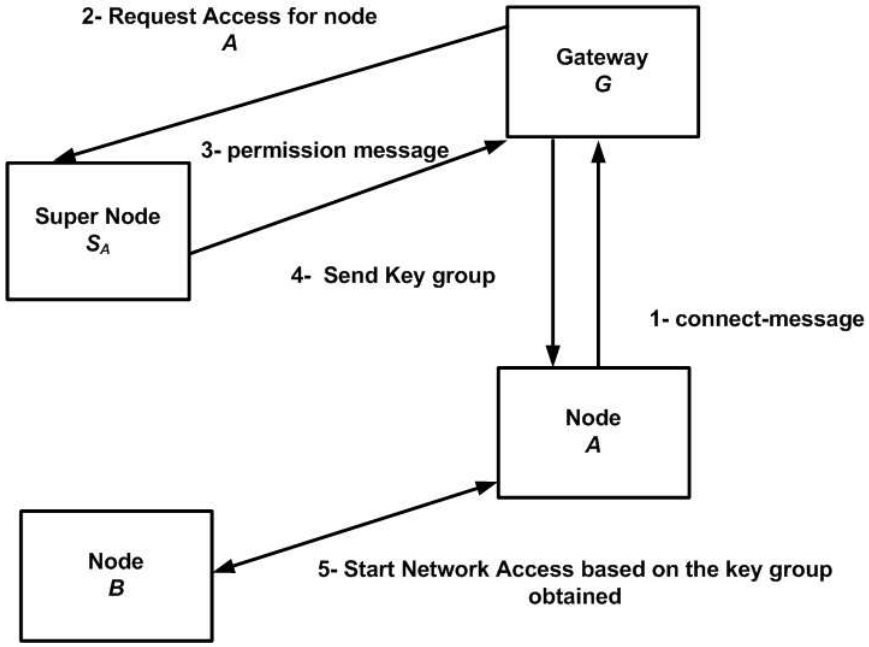

Figure 6.2: Granting network access for node A over network supervised by gateway G.

size n is a concatenation of n key:

$$KG_n \leftarrow k_x \mid k_{x-1} \mid \ldots \mid k_{x-n+1}.$$

To reduce the message size, the gateway does not need to send all the keys in the key group, but only the last key K_{x-n+1} in the group and the group length. The node can generate the group by consecutively applying the hash function. The gateway generates the network access message by encrypting the key group with the node public key:

$$AccessMessage \leftarrow E_{PK_A}(KG_n \mid TimeStamp).$$

After verifying the access message and the permission message, the node gets the key group and starts communicating over the network.

It should be noted that the node can generate all the keys that precede the first key in the key group (using the hash function). It is expected that the messages already circulating in the network are encrypted using previous keys, so that the node can verify the validity of these messages. The node cannot generate any key for a future time period using the key group based on the one-way key chain properties. For example, the node that received a key group KG_n with current key K_x can generate any previous key K_i where $L-1 \geq i > x$. If a node needs to communicate over the network after the expiry of its key group, it should re-register with the gateway.

After obtaining the key group, the node can start communicating with other nodes. When the node wants to send a message, it needs to generate a MAC block using the current network key and forwards it to neighbor nodes (based on the routing technique applied). The message exchanges are in the form of

$$\begin{aligned} ExchangedMsg &\leftarrow msg \mid TimeStamp \mid MAC, \\ MAC &\leftarrow HMAC_{K_x}(Msg \mid TimeStamp). \end{aligned}$$

When an intermediate node receives a message, it checks the MAC block and then stores the message to be forwarded. The intermediate node is not able to disclose the message contents because the message, msg, should already be encrypted with another key shared between the source and the destination to achieve end-to-end secure communications, as discussed in Section 6.4.

To prevent any node from continuing the communication with a previously granted key group, messages sent with expired keys are discarded as follow: Key K_i has a time frame $[t_x, t_x + t_{key}]$ and each message has a $TTL = t_{message}$. If a message at time $t > t_x + t_{key} + t_{message}$ is authorized with key K_i, it will be discarded.

With the proposed approach, a message sender needs to perform one sym-

metric key encryption per message. Each intermediate node also needs to perform one symmetric key decryption per message. Intermediate nodes store the original message (if valid) for future forwarding. They do not need to re-compute the message MAC when forwarding the message.

6.4 End-to-end Message Security

The importance of message security in a DTN environment is due to the difficulty to control the message route or to trust the intermediate nodes. A message may be routed through a malicious node, which can disclose and/or change the message contents. A message receiver needs to authenticate the sender identity and the contents of the message. Also, the message sender needs to authenticate the message's receiver and to ensure that only the receiver can decrypt the message contents. In regular networks, a mutual authentication between the sender and the receiver is performed before a secure end-to-end path is established for communications. The mutual authentication requires the presence of a trusted third party (*e.g.*, certificate authority) to perform the mutual authentication phase between the communicating parties.

Regular techniques cannot be applied directly to a DTN environment due to the potential unavailability of a physical end-to-end path either between message's sender and the receiver or between any of them and a trusted third party. Moreover, without available communications with a trusted third party, the two communicating parties are not able to authenticate each other in a timely manner to allow the communication. There are some adaptations of regular techniques to handle this problem within a DTN which are discussed next.

6.4.1 Related Work

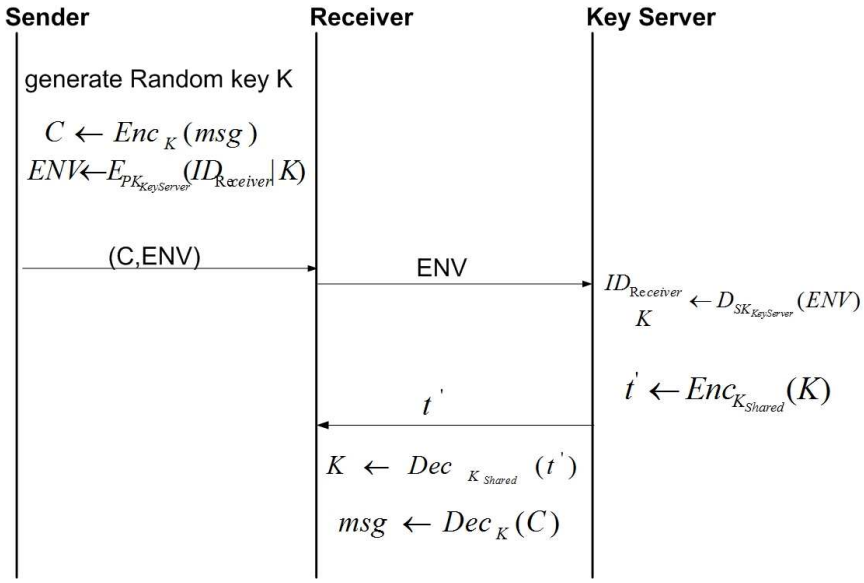

Figure 6.3: Traditional public key cryptography for DTN [118].

The traditional public key cryptography technique encounters, over a DTN, the problems of unavailability of communications with the trusted third party and limited node ability to use asymmetric encryption due to power constraints. In [118], an approach is proposed to cope with the problems by i) minimizing the number of required contacts with the trusted third party, and ii) moving part of asymmetric decryption operation to the third party to minimize the overhead imposed on the receiver. Figure 6.3 shows the scenario introduced in [118]. The sender of message msg picks any random key K and generates the cipher text C. The sender generates an envelope ENV using the key server's (*i.e.*, the trusted third part) public key that encloses the used secret key, and

sends both C and ENV to the receiver, given by

$$\begin{aligned} C &\leftarrow Enc_K(msg) \\ ENV &\leftarrow E_{PK_{KeyServer}}(ID_{Receiver}|K). \end{aligned}$$

In order to extract the key from the envelope to decrypt the cipher, the receiver sends the received envelope to the key server. The key server decrypts the envelope to recover the key and sends the key back to the receiver encrypted with a previously shared key K_{Shared} with the receiver. The receiver recovers the key and the original message as follow:

$$\begin{aligned} ID_{Receiver}|K &\leftarrow D_{SK_{KeyServer}}(ENV) \\ t^{'} &\leftarrow Enc_{K_{Shared}}(K) \\ K &\leftarrow Dec_{K_{Shared}}(t^{'}) \\ msg &\leftarrow Dec_K(C). \end{aligned}$$

There are several advantages of the approach: It overcomes the need for certificate validation and revocation by forcing the shared key disclosure through the key server; It moves receiver's identity authentication to the key server. On the other hand, it does not handle the sender's authentication, which can be solved by adding the sender's identifier and a signature (with the key shared between the sender and the key server) to the envelope. The sender still needs to perform asymmetric encryption to send the shared key to the receiver. The approach will cause received messages' decryption to be delayed until a contact occurs with the key server.

Identity Based Cryptography (IBC) [123] is a cryptographic method which enables message asymmetric key encryption and signature verification using a public identifier of the receiver as the receiver's key. This technique uses a

commonly trusted node as the private key generator (PKG). The PKG has a public parameter PP and its correspondence secret key SK_{PKG}. The public identifier can be, for example, a web address or an email address. The PKG can generate a private key SK_A for any user A with public identifier ID_A. Before generating a private key based on the user's public identifier, the PKG must verify that the user is allowed to use this identifier for secure communications. A user, A, signs any outgoing message with the private key SK_A. The message receiver verifies the signature using the sender's public identifier ID_A and PP. Messages intended for user A are encrypted using ID_A and PP, so that only user A can decrypt them with the secret key SK_A.

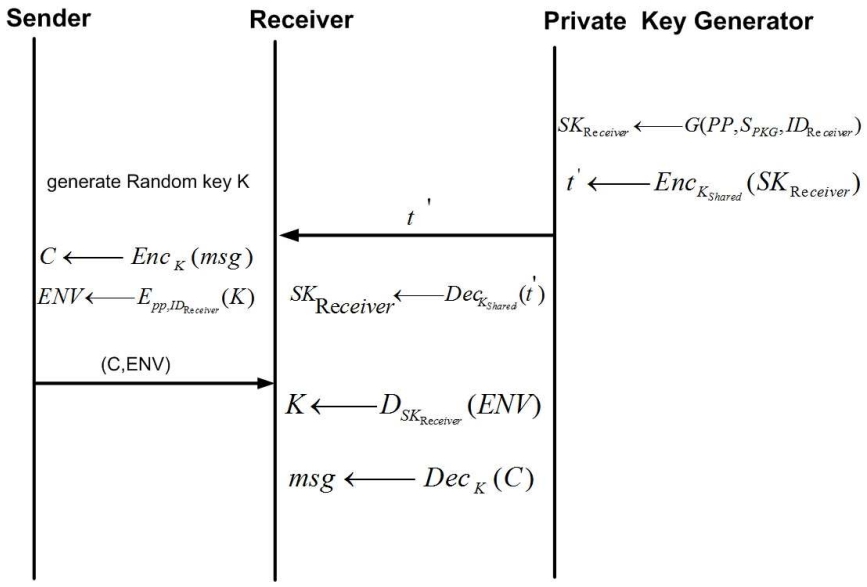

Figure 6.4: Identity based cryptography for DTN [118].

Figure 6.4 shows a scenario suggested in [118] for secure communications between two nodes over a DTN using IBC. For message, msg, the sender picks a random key K for symmetric encryption and generates a cipher text C and

an envelope ENV:

$$\begin{aligned} C &\leftarrow Enc_K(msg) \\ ENV &\leftarrow E_{PP,ID_{Receiver}}(K). \end{aligned}$$

The sender sends both C and ENV to the receiver. The receiver decrypts the original message from the cipher text after extracting the shared secret key from the envelope using the private key associated with its public identity used. The receiver gets the key information out of the envelope and extracts the original message as follows:

$$\begin{aligned} K &\leftarrow D_{SK_{Receiver}}(ENV) \\ msg &\leftarrow Dec_K(C). \end{aligned}$$

The PKG generates the private key associated with the receiver's public identifier. It uses a secret key K_{Shared} already shared with the receiver to make a secure message $t^{'}$ containing the generated private key. The PKG then sends the message to the receiver which extracts the private key as follow:

$$\begin{aligned} SK_{Receiver} &\leftarrow G(PP, SK_{PKG}, ID_{Receiver}) \\ t^{'} &\leftarrow Enc_{K_{Shared}}(SK_{Receiver}) \\ SK_{Receiver} &\leftarrow Dec_{K_{Shared}}(t^{'}). \end{aligned}$$

In this scenario, the receiver can independently receive the associated private key from the PKG. If the receiver does not already have the private key, the received message decryption will be delayed until a communication opportunity with the PKG occurs.

The main advantage of IBC over the traditional public key cryptography is the use of node public identifier as the node public key, which removes the

necessity of contacting the trusted third party to verify node certificate (*i.e.*, checking node authenticity). However, the problem of updating and revoking these certificates (*i.e.*, public/private key pairs) still exists in this scenario. This is solved in [124] by periodically refreshing the node public identifier and hence its private key, where the node public identifier is made by combining a long lived identifier with a description of the validity period (*e.g.*, a day). For example, `hsamuel@uwaterloo.ca:18-08-2010` refers to the public identifier that *hsamuel* can use for encrypting the messages on *August* $18, 2010$. A key holder should periodically contact the PKG to receive updated keys. The IBC solves the problem of sender and receiver authentication without the need to contact a trusted third party. However, it is argued in [102] that the checking of the public parameter PP is equivalent to verifying the certificate in traditional public key cryptography. Moreover, the IBC does not solve the problem of limited node power to cope with asymmetric key cryptographic operations for message security.

Both traditional public key cryptography and IBC techniques can be adapted to suit the super nodes system by letting node's super node play the role of key server or PKG. However, using these techniques requires roaming nodes to extensively perform asymmetric key cryptographic operations. Moreover, traditional public key cryptography imposes a long delay on received message decryption due to the potential long disconnections to the node. Next, we propose a technique that depends mainly on symmetric encryption to reduce overhead and uses the idea of key chains to achieve timely updates for node keys.

6.4.2 The Proposed Security Approach

Preventing unauthorized users from sending their messages over the network does not implies the confidentiality of exchanged authentic messages. Any malicious node that receives a message for forwarding can expose the message contents. Due to the inability to control the message forwarding route within the system under consideration (especially for an unstructured open network such as MANET), secure end-to-end message exchanges are mandatory.

In the system under consideration, the existence of super nodes that can communicate reliably and securely over the Internet backbone offers an advantage to relax the constraints of end-to-end secure message exchanges. The main idea is to use the super node as a node delegate that performs the mutual authentication and key sharing on behalf of the mobile node. Under the super-node architecture, there are two communication scenarios for node-to-node message exchanges: 1) the message sender and receiver can find a physical end-to-end path, and 2) a physical end-to-end path cannot be established, so that messages are routed through the destination's super node. In both cases, the source node should contact the destination's super node. For the first case, the source node has to contact the destination's super node to locate the destination, while in the second case all messages are sent through the super node.

Secure Communications between Node and Super Node

We propose to use symmetric encryption to ensure information security for communications between a node and its super node. All message exchanges are encrypted using a shared secret key, which reduces the overhead imposed by asymmetric key cryptography based techniques. The shared key is updated periodically to prevent its exposure. Updating the shared key requires hand-

shaking between the node and its super node, which is challenging with the expected node's frequent long disconnections. To handle key updates, a key chain is shared between the node and its super node. The key chain is used for a period of time which is divided into time frames of equal length and, for each time frame, a specific key from the chain is used to secure the communications. At the end of a time frame, both the node and its super node update the shared key to the next key from the key chain without the need of any handshaking between them. After all the keys from the chain are used, a new key chain will be generated and shared between the node and its super node. This technique does not need to include the secret key in the exchanged messages as in traditional asymmetric cryptography based techniques. Asymmetric key cryptography is used only during the chain initialization to securely exchange the key chain and to allow the communicating parties to authenticate each others, as discussed next.

Figure 6.5 shows the proposed procedure for establishing secure communications between a node, A, and its super node S_A. When a node, A, is connected through an access network, it sends a connection message to its super node to update the super node with its current location and to be granted the privilege to access the access network resources as discussed in Section 6.3. If there is no shared key chain or a previously shared chain expired, node A initializes a new chain by generating a random key as the chain seed value K_0 and length L. The node prepares the connection message as:

$$\begin{aligned} ConnectMsg &\leftarrow ID_A \mid ID_{net} \mid E_{PK_{S_A}}(K_0 \mid L) \mid TimeStamp \mid SIG_A, \\ SIG_A &\leftarrow E_{SK_A}(H(ID_A \mid ID_{net} \mid E_{PK_{S_A}}(K_0 \mid L) \mid TimeStamp)). \end{aligned}$$

The access network identifier ID_{net} is to inform the super node of its current

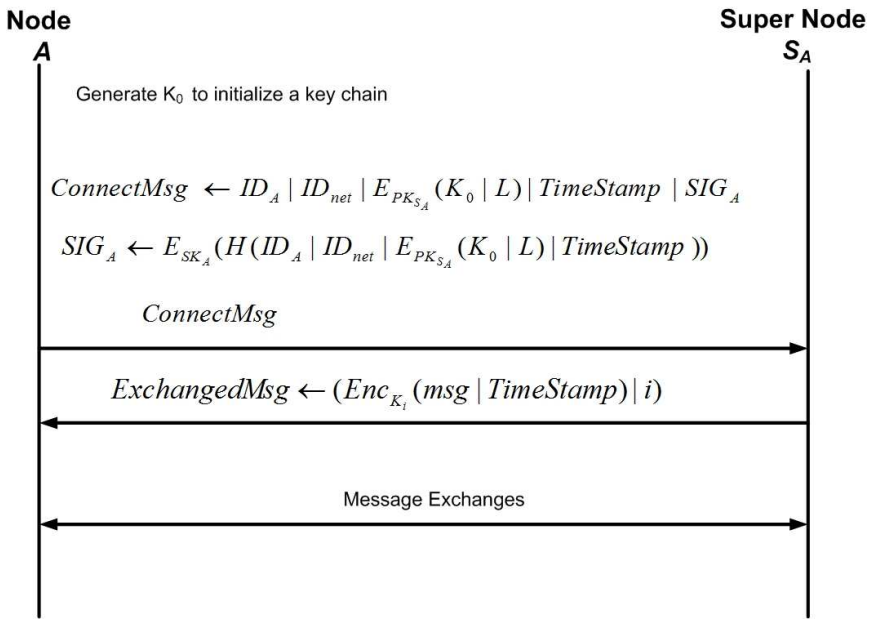

Figure 6.5: Secure communications between a node and its super node.

location. The connection message contains a time stamp field to prevent a reply attack. The key chain information is encrypted with the super node public key to ensure that only the super node can decrypt this information. The node signs the message with its private key to enable the super node to authenticate the sender identity. The super node verifies the connection message and initializes the key chain. The super node sends access information to the node as discussed Section 3.2. The node and its super node can start exchanging messages secured with the current shared key, K_i, from the shared key chain:

$$ExchangedMsg \leftarrow (Enc_{K_i}(msg \mid TimeStamp) \mid i).$$

The node does not have to initialize a new key chain until all the keys in the current key chain are used. This allows the node to be disconnected from its super node while keeping an up-to-date shared key without any handshaking

between them.

Due to the expected delay in message delivery, messages may not be delivered in sequence. Hence, the receiver (i.e., the node or its super node) may receive messages encrypted with the keys out of order, or with previous keys other than the current key. The proposed technique addresses this potential problem by including a time stamp in the message. The receiver accepts the message as long as the key index matches the enclosed time stamp.

Securing Node-to-Node Communications

To establish a secure end-to-end message exchange between two nodes, our proposal is to use the destination node's super node as the destination's delegate. This moves the mutual authentication process from the communicating nodes (where the communication is challenged) to their super nodes (where the communication is reliable and secure). The first step for communications between two nodes is that the source node inquiries about the destination node location from the destination node's super node. This step can be used to enable the destination super node to authenticate the source node identity. The destination super node issues a permission for secure communication in the form of an access ticket that the source node can use to communicate with the destination node. With the access ticket, the destination node does not need to re-authenticate the source node as the ticket proves that the sender is authenticated by the destination super node. Moreover, the source node does not need to authenticate the destination node because the destination node is the only one who can extract the shared key information from the ticket.

Figure 6.6 shows the proposed procedure to establish a secure end-to-end message transfer between two nodes. Suppose that node B wants to start a

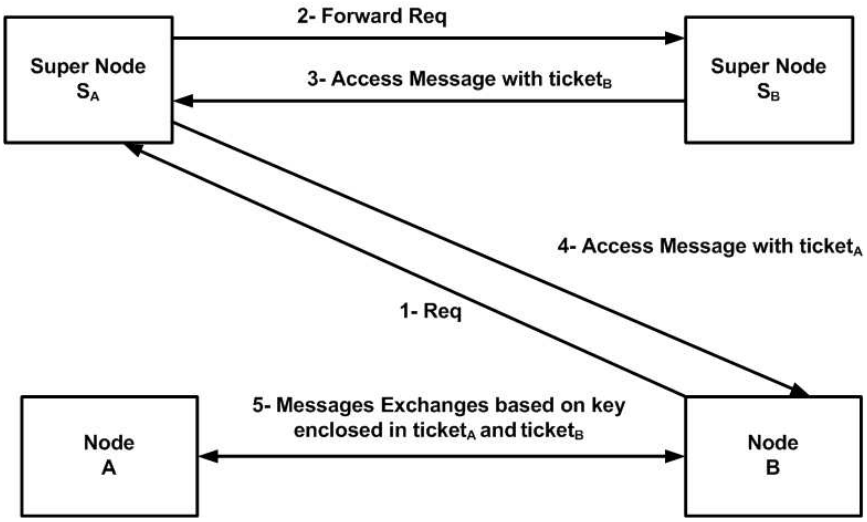

Figure 6.6: The procedure to establish an end-to-end secure message exchange.

secure communication with node A. Node B locates the super node S_A and sends a communication request, Req, to S_A as follow:

$$Req \leftarrow (ID_A \mid ID_B \mid TimeStamp \mid \underbrace{i \mid Enc_{K_i}(ID_A \mid ID_B \mid TimeStamp)}_{AuthenticationPart}).$$

The authentication part in the request message is encrypted by the current shared key between node B and its super node. If S_A is not the super node of node B, it cannot authenticate the sender identity. As a result, it forwards the request message to node S_B (based on the assumption that super nodes can communicate reliably and securely over the Internet backbone). Node S_B verifies that node B is the sender of this message based on their shared key chain and generates *access ticket*, $ticket_B$, to S_A for a secure communication with node B. Super node S_B replies to S_A with an access message that is secured based

on the assumed existing secure connection between the super nodes:

$$\begin{aligned} ticket_B &\leftarrow i \mid Enc_{K_i}(ID_A \mid ID_{S_A} \mid K_B \mid TimeStamp \\ &\quad \mid ExpirationTime), \\ AccessMsg &\leftarrow K_B \mid ExpirationTime \mid ticket_B. \end{aligned}$$

The access ticket $ticket_B$ can be used only by node A and/or its super node S_A, which is declared as a part of the ticket. The ticket also contains a randomly generated secret key K_B to secure the communications with node B. The ticket is valid for a period of time determined by $ExpirationTime$ field. The access ticket $ticket_B$ authenticates both nodes A and S_A identities to node B. When S_A receives the access message that confirms the identity of node B, it generates an access ticket ($ticket_A$) using the current key, K_j, from the key chain shared with node A. Super node S_A sends an access message to node B that contains node A location and $ticket_A$:

$$\begin{aligned} ticket_A &\leftarrow j \mid Enc_{K_j}(ID_B \mid ID_{S_B} \mid K_B \mid TimeStamp \\ &\quad \mid ExpirationTime) \\ AccessMsg &\leftarrow Location_A \mid ticket_B \mid Enc_{K_B}(ExpirationTime \mid ticket_A). \end{aligned}$$

When node B receives the access message, K_B can be extracted from the ticket $ticket_B$ using K_i. Node B can start communicating with node A or its super node (if no end-to-end path exists). Each message msg sent from node B to node A is encrypted using the shared key K_B. An exchanged message includes the encrypted message and the access tickets, given by

$$ExchangedMsg \leftarrow Enc_{K_B}(msg) \mid ticket_A \mid ticket_B.$$

When node A receives the message, it checks $ticket_A$ using K_j, and then it decrypts the message using K_B obtained from the ticket. Note that, unlike the

previous techniques [118], a message receiver does not need to authenticate the message sender and it can decrypt the message without any delay or asymmetric cryptography overhead. Moreover, node A can reply to node B using $ticket_B$ so that the communication proceeds without any need to contact the super nodes again for authorization.

To prevent using expired tickets in communications, messages sent with expired tickets are discarded as follow: Given that the ticket expiration time t_{ticket} and each message has a $TTL = t_{message}$, if a message using this ticket is received at time $t > t_{ticket} + t_{message}$, the message will be discarded.

A main challenge for authentication over DTN is the delay required for handshaking to complete the authentication process. In our scheme, the delay is minimized by using the mandatory message sent to the super node to locate the destination node. As a result, the sender does not need to send a separate message for authentication. Moreover, within the lifetime of the issued ticket, the sender does not need to re-send an authentication message for each message. Note that there exist some research efforts to provide a self organized authentication without the need to contact a trusted third party, such as the work in [125]. The technique is based on the self signed certificates issued by the nodes themselves. A main concern for the technique to be adapted to the super node architecture is the size of required certificate repositories within each node, taking into consideration the large size of the interconnected networks. The authentication requires processing a graph of the intersection among the node certificate repositories, which can be very large for roaming nodes with a possibility of no shared certificates. With the expected unavailability of the communicating nodes and/or an end-to-end path, the handshaking required for the authentication (*i.e.*, to exchange the certificates) can either cause a long delay for the communication or prevent the communication completely. As it is

the responsibility of the nodes to authenticate each other, the existing technique imposes a processing overhead to all the nodes.

6.5 Performance Evaluation

We extend the simulation experiments introduced in Section 4.6 as follows. We study how the proposed security schemes affect system performance under two different routing techniques: the epidemic routing and the dominating set (DS) based routing. In the epidemic routing, each node forwards a message to all its neighboring nodes, in anticipation that one of these nodes may meet with the destination node in the near future as it roams. This may be inefficient in terms of network resource usage, however it is sometimes necessary. On the other hand, the DS routing limits the number of forwarded messages required to deliver a message by limiting the number of nodes to which the message should be forwarded by a node. The DS routing counts on forwarding the message only to the DS members, which are nodes that have a high probability to meet with all the other nodes in the network. We compare the performance of the proposed authorization techniques with that of the system with no authorization. The performance is measured in terms of (1) the number of forwarded messages over the network to demonstrate how efficiently each technique uses the available resources (*e.g.*, radio spectrum bandwidth), and (2) the number of undelivered authorized messages to indicate how reliable the technique is in delivering authorized messages. We compare the two proposed security techniques in terms of the number of asymmetric key cryptographic operations to measure how efficient the intermediate node computing power is used, with an increasing number of forwarded messages.

In our experiments, the MANET coverage area is a square of size 10×10

partitions. Each simulation proceeds in discrete time steps. There are 50 mobile nodes with mobility trajectories independent of each other. For each simulation run, a transition matrix $\mathbb{M}$ is randomly generated and stays fixed till the end of the simulation. Initially, the node locations are uniformly distributed over the service area. As the simulation time increases, each node (if connected) moves randomly according to the transition matrix. When a node moves to a new partition, it stays there for a residence time that is an exponential random variable with an average of 20 simulation steps. At the end of the residence time, the node moves to a new partition with a probability of 0.7, or disconnects from the network with a probability of 0.3. If the node disconnects, it will stay disconnected for a duration that is exponentially distributed with an average of 20 time steps. For simplicity, we assume that a node is able to communicate only with other nodes in the same partition. Messages are generated based on a Poisson process with mean rate of $\frac{10}{3}$ messages per time step. The source and destination mobile nodes for each message are selected at random. All the messages are equal in size, with the same message time to live of 40 simulation steps. The buffer space is 15 messages at each mobile node and 2000 messages at the gateway. When the node buffer is full and a new message is received, the oldest message in the buffer is removed to accommodate the new message. Moreover, 20 percent of the nodes are unauthorized to use the network resources. They are assumed to behave honestly in carrying and forwarding messages from others. In addition, they generate their own messages and try to inject them to the network.

At the start of simulation, all the nodes generate a request message to the gateway to gain access to the network based on the proposed security scheme (*i.e.*, they receive a certificate in the first approach or a key group in the second approach). All the nodes are granted the same access period for simplicity in

simulation. When the access period of a node expires, the node has to re-request access from the gateway. At each time step, the node detects its neighbor nodes and exchanges the buffered messages with them (the messages that the neighbor nodes do not already have) based on the routing technique. Each node also updates its buffer by removing expired messages. For each experiment, a communication scenario (i.e., set of messages, user connections, user disconnections, user movements) is set up randomly and run for each scheme.

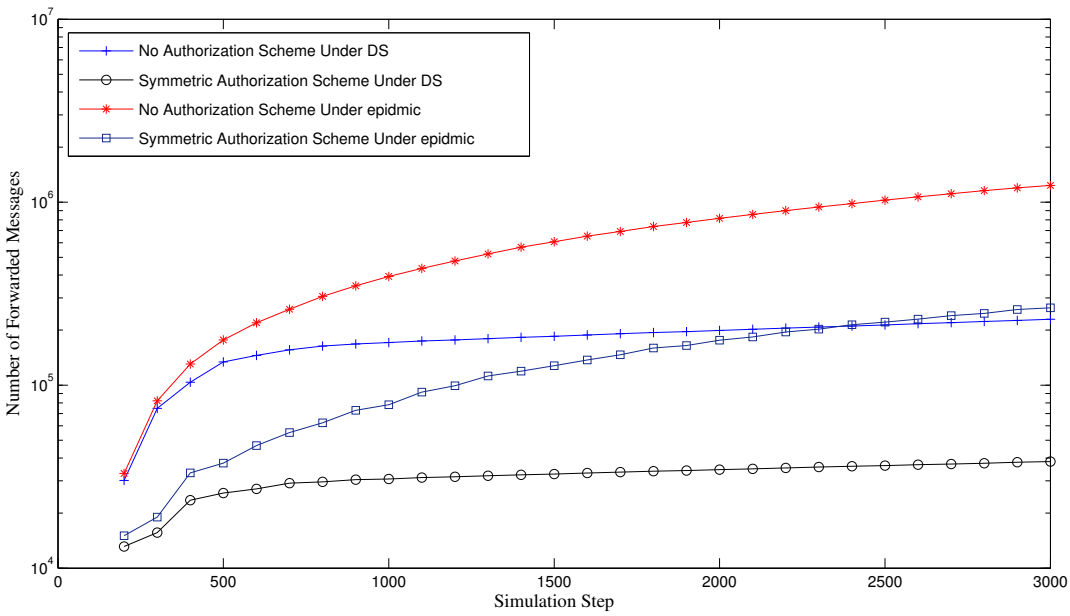

Figure 6.7: Comparison of the proposed authorization schemes in terms of the number of forwarded under the DS and the epidemic routing.

Figure 6.7 shows a comparison between the case of applying no authorization scheme and the case of applying the proposed symmetric key cryptography based authorization scheme under the epidemic routing and DS routing, in terms of the total number of forwarded messages. It is clear that, with the existence of unauthorized traffic, the authorization scheme is important to reduce the

number of forwarded messages. This applies to both routing techniques under consideration. Moreover, the number of lost (undelivered) authorized messages is increased in the case of no authentication, as shown in Figure 6.8. This is mainly due to the limited buffer space at intermediate nodes which have to drop old messages when buffer overflow occurs. With an increased number of unauthorized messages, the probability of dropping authorized messages increases.

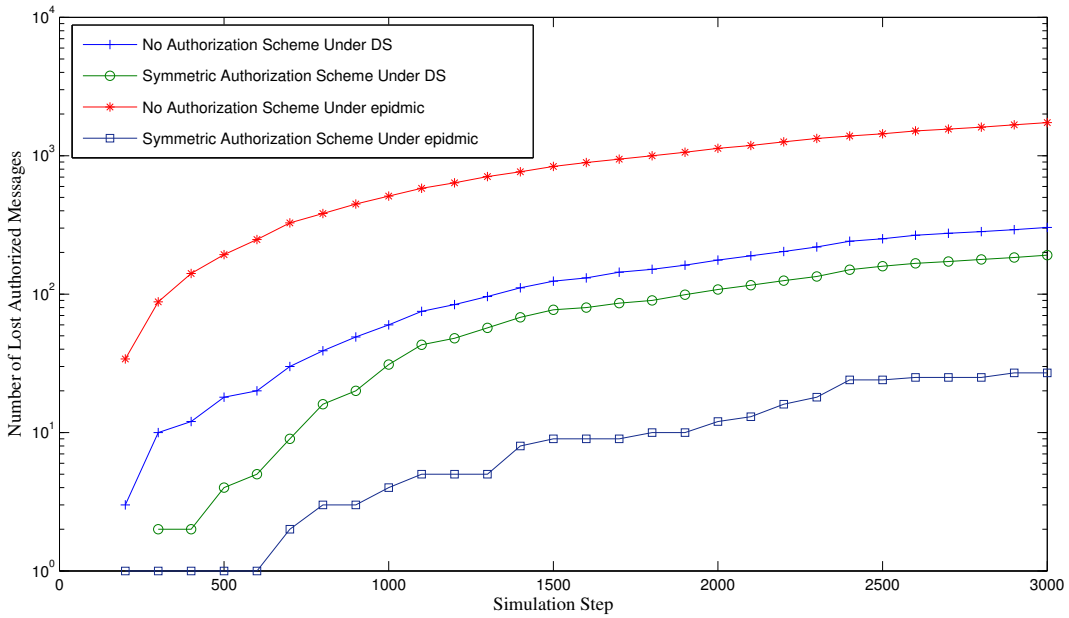

Figure 6.8: Comparison of the proposed authorization schemes in terms of the number of lost authorized messages under the DS and the epidemic routing.

Both of the proposed authorization techniques perform equally in terms of the numbers of forwarded messages and lost messages. However, when comparing them regarding the number of asymmetric key cryptographic operations, it is clear that the symmetric key based cryptography outperforms the asymmetric key cryptography based scheme under the routing techniques, as shown in Figure 6.9. It should be noted that the symmetric key cryptography based scheme

does not eliminate the usage of asymmetric key cryptographic operations as a node has to perform asymmetric key operation to request network access and to receive the key group (if access granted), as discussed in Section 6.3.2. However, with a larger network size (in terms of number of nodes) and/or a shorter granted access period per node, even though the symmetric key cryptography based scheme increases the number of the required asymmetric key cryptographic operations (that are required for messages sent at connecting, and for initializing the key chain), it still outperforms the asymmetric key scheme. As a result, it is expected that the symmetric key cryptography based technique always outperforms the asymmetric key cryptography based technique in terms of the number of asymmetric key cryptographic operations under all conditions.

Comparing the performance of the two routing techniques under the proposed authorization scheme, Figure 6.7 shows how the DS routing outperforms the epidemic routing in terms of the number of forwarded messages, which is consistent with the observation in the absence of unauthorized traffic. In the presence of unauthorized traffic, even without the authorization, the DS routing outperforms the epidemic routing, as the DS routing limits the number of nodes that a message should be forwarded to. On the other hand, Figure 6.8 shows that, with the authorization scheme in place, the epidemic routing outperforms the DS routing in terms of the number of lost authorized messages. With the DS routing, a message is more likely to be expired before a contact occurs between a message carrying node and the next DS member. However, the number of lost authorized messages under the DS routing and the authorization scheme is much smaller than that under either the epidemic routing or the DS routing without the authorization scheme.

Considering the number of asymmetric key cryptography operations, the DS

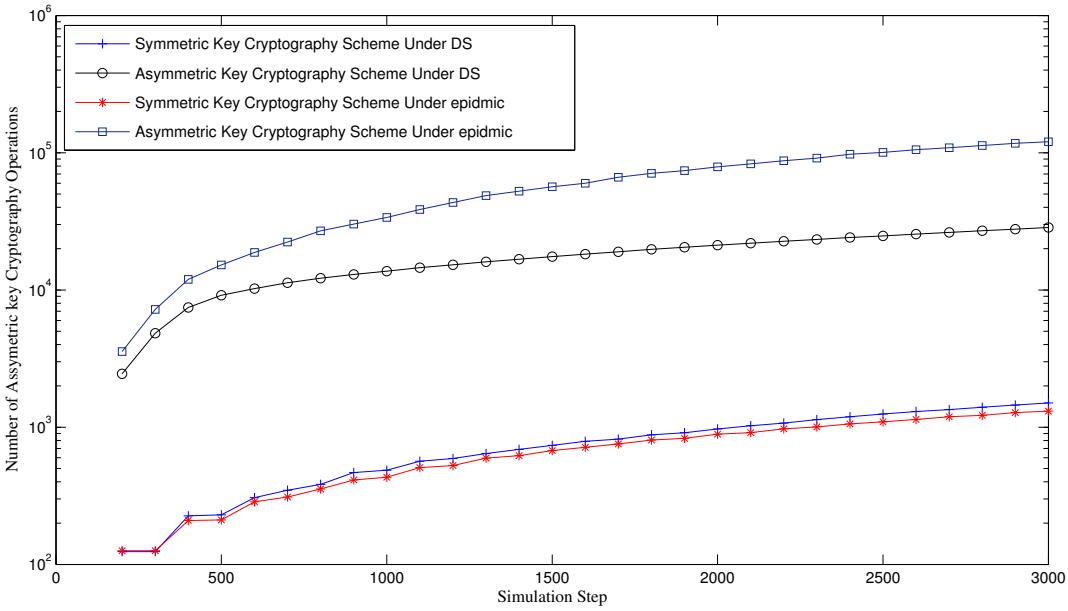

Figure 6.9: Comparison of the proposed authorization schemes in terms of the number of asymmetric key cryptography operations under the DS and the epidemic routing.

routing outperforms the epidemic routing, when asymmetric key cryptography based scheme is employed, as shown in Figure 6.9. This is because the number of asymmetric key cryptography operations is related to the number of message forwarded in the asymmetric key cryptography based scheme. However, the epidemic routing and DS routing perform similarly in terms of the number of asymmetric key operations performed, when the symmetric key cryptography based scheme is employed. This is due to the fact that the number of asymmetric key operations in this case is proportional to the number of connection messages and permission messages sent over the network. The higher number of lost messages in the DS routing likely results in more lost connection messages and/or permission messages, which requires the recalculation and resending of these messages.

We have carried out extensive simulations to evaluate the performance of the proposed schemes. The main observations can be summarized in the following: (a) Both schemes introduce an extra delay for a newly connected node to be able to communicate in the network. This delay accounts for the time for the access request to reach the gateway and the time for the node to receive the access grant information (key group or certificate). However, even with a highly sparse network, the simulation results show that the delay can be neglected when compared with the node connection time for the system model under consideration; (b) Both proposed schemes introduce extra cost as compared with the case of no authorization procedure. This cost is in the form of extra message exchanges to request and grant node access and the delay that a node encounters for accessing the network. This cost becomes obvious with a very low percentage of unauthorized messages. However, the overhead imposed by an increase in unauthorized traffic makes the extra message exchanges totally negligible; (c) When a node needs to extend its network access period, it sends

a request message to the gateway. This introduces a delay until the response is sent back. The delay can be eliminated by requesting access in advance before the current access period is expired. The advance period can be estimated based on the average message delay that a node encounters in contacting the gateway.

6.6 Related Work

6.6.1 The ZigBee Network

An interesting security technique related to our proposed scheme is implemented in the ZigBee networks. ZigBee^{TM}is a registered trademark for the ZigBee alliance [127], which is a group of companies that maintain the ZigBee standard. The ZigBee standard defines a set of protocols for short-range wireless networks with low-data-rate, built over the IEEE 802.15.4 layers [126]. The IEEE 802.15.4 standard is developed, independently of the ZigBee standard, for low-rate wireless personal area networks (LR-WPANs). ZigBee is designed mainly to provide support for applications that require a low data rate, long battery life, and secure networking. As a result, the ZigBee standard is suitable for systems such as sensor networks.

The ZigBee standard uses symmetric key cryptography for message authentication and encryption, based on the AES with 128 bit key [126]. It introduces the concept of using a device as a trust center. The trust center stores the keys for a network and authorizes other devices to join the network. A network key is defined for message authentication over the network. This key should be globally shared for all nodes authenticated to use the network. The trust center specifies the current network key and sends the updates to authorized devices to authenticate their messages over the network. If two devices need to

communicate securely over the network, they share another key, called link key in the standard. This key is used for point-to-point secure communication.

The network access scheme employed within the ZigBee standard introduces an approach similar to our symmetric key based scheme. It uses a network key to authenticate exchanged messages in order to prevent unauthorized nodes from communicating over the network. However, the ZigBee security technique does not address network access revocation for a specific node. This is addressed in our scheme by allowing the node to have access to a subset of the network generated key chain (*i.e.*, key group). The way to revoke access from a specific node within the ZigBee system is to make the trust center update the network key and inform all other network nodes. Moreover, a major difference is the implicit assumption in the ZigBee standard that all the nodes are connected and can access the trust center. The trust center can update the network key and propagate this update to all the connected nodes immediately. This assumption cannot be satisfied for the DTN system under consideration. On the other hand, our technique allows nodes to be able to communicate and update the network keys even if the trusted third party (*i.e.*, the gateway in our system and the trust center in the ZigBee system) is unreachable.

Another main difference between the ZigBee security technique and our aproach is the inability of the ZigBee security technique to tolerate a long delay. In a ZigBee network, a newly joined node does not need to know the previous network keys. This is because it is expected that no old messages should be circulating for long in the network. As a result, this technique cannot be applied to the DTN system under consideration without a technique to let a new node authenticate messages already existing in the system. This is achieved in our scheme by allowing a newly joined node to generate all previous keys in the used key chain.

6.6.2 Lightweight Certificates

Previous techniques introduced in [128–130] address the overhead problem induced by the asymmetric key cryptography authentication techniques over wireless networks, where nodes have limited processing power and storage capacity. These techniques are proposed to replace regular PKI certificates with symmetric key cryptography based certificates. Here we briefly review the techniques and then discuss why these techniques cannot be applied to our problem domain.

In [128], the TESLA protocol [122] is extended to generate symmetric key based certificates. This technique is based on the existence of a globally trusted certificate authority (CA). The CA generates a one-way key chain to be used over a long time period, where at time frame i the used key from the key chain is denoted by K_{CA_i}. A node, B, that wants to authenticate its identity to other nodes at time frame n, contacts CA with their pre-shared symmetric key $K_{CA,B}$. The CA generates authentication key K_{B_n} to node B to authenticate its messages starting from the time frame n. It creates a certificate $Cert_{CA_n}(B)$ that binds the key K_{B_n} to node B at time frame n using its key from the generated key chain to be used at the time frame n, as follows:

$$\begin{aligned} Cert_{CA_n}(B) \;\leftarrow\; & ID_B \mid Enc_{K_{CA_n}}(K_{B_n}) \mid n \;+\; d \\ & \mid HMAC_{K_{CA_n}}(ID_B \mid Enc_{K_{CA_i}}(K_{B_n}) \mid n \;+\; d) \end{aligned}$$

where $d > 0$ *and* $(n + d)$ is the time frame when the key K_{CA_n} will be disclosed to the network. Node B can use the issued certificate and the issued key K_{B_n} to authenticate any message it sends over the period $[n, n + d]$. Any node receiving a message from B should buffer it until the key K_{CA_n} is announced by the CA at the time frame $(n + d)$. The main assumption for the technique to work is that the CA can send its announcement to all the network nodes immediately and reliably. When the key K_{CA_n} is known to all the nodes, the key K_{B_n} can be

extracted from the certificate and the buffered messages can be authenticated by the receivers. Starting from the time frame ($n + d$), no message can be authenticated using the key K_{B_n}. Node B should request a new certificate for further communications.

In [129], the technique introduced in [128] is extended for implementing an authentication framework within sensor networks to authenticate nodes to base stations. In [130], a variation of the technique is proposed so nodes share a one-way key chain instead of single key. A node uses its issued certificate key as anchor for a generated key chain. The node uses the rest of the key chain to communicate with nodes that received and verified the certificate. However, the node still needs to request a new certificate if it wants to communicate with other nodes that have not verified the certificate.

The main similarity between these techniques and our proposed technique is the use of symmetric key cryptography and key chains for authenticating messages sent by a node. The main drawback of these techniques is their time sensitivity. These techniques assume continuous communication between the certificate authority and all nodes over the network. The work in [130] assumes this communication is accomplished through a satellite link to achieve continuous availability of the certificate authority. Due to the expected long delays and the expected unavailability of continuous communication with the certificate authority, the key exposure is not expected to occur in a timely manner. This problem makes these techniques not useful within our problem domain.

PKI Lightweight Certificates

Public key management is an open problem for DTN security [102] due to the DTN characteristics. The main challenge for applying existing public key cer-

tificate management methods in DTNs is how to efficiently revoke an unexpired certificate, considering the long communication delays and node limited storage and communication capabilities. In the bundle security specification [102], a recommendation is made to use short-time certificates to avoid the certificate revocation problem. We use this technique in our solution introduced in Section 6.3.1.

Other research efforts in the DTN security area try to address the public key certificate management problem through implementing an efficient CRL mechanism. In [114], the problem is addressed by using epidemic routing to periodically distribute the CRL. Moreover, a technique based on bloom filters is employed to reduce the storage and transmission needed to make the CRL distribution efficient. Recent research efforts address the problem of designing a lightweight certificate for wireless network devices with limited capabilities (in terms of computing power, and transmission bandwidth). In [131], a technique is proposed to reduce the certificate size. Also, in [132], the certificate revocation problem is addressed by trying to find an efficient revocation method for certificates in VANETs.

ECQV (Elliptic Curve Qu-Vanstone) Implicit Certificate Scheme [133] is a new promising technology for implementing lightweight PKI certificates using ECC. A traditional PKI certificate binds a public key to an entity ID through a digital signature of the certificate authority, which can be denoted as explicit binding because of the existence of an explicit signature. On the other hand, an implicit certificate does not include an explicit signature of the certificate authority to achieve binding. Instead, it uses a public reconstruction value generated by the entity and the certificate authority together. Other nodes can compute the entity public key from the public reconstruction value. ECQV implicit certificate, with considering the key small size for ECC, can achieve a

significantly smaller certificate size when compared with traditional certificates that use explicit biding. Moreover, the signing and verification mechanism employed with ECQV, with considering proper hardware implementation of ECC, can achieve more efficient computing certificates, as compared with the regular certificates. With a proper definition of a certificate revocation mechanism, ECQV certificate can be a very good choice for PKI certificates within a DTN environment.

Adapting a PKI lightweight certificate management mechanism within the super node system is a very interesting topic that needs further research, as introduced in Chapter 7.

6.7 Summary

This chapter mainly investigates how to limit unauthorized traffic within a MANET as a major component of the super node system. The proposed schemes are mainly adjusted to fit delay tolerant network based MANETs that serves as access networks within the super node architecture. We adopt traditional public key infrastructure (PKI) based certificates to solve the problem under consideration. We also propose a new technique based on an idea of separating the message authorization and message sender authentication at intermediate nodes. The new technique uses symmetric key cryptography to reduce the overhead from that when using asymmetric key cryptography. We discuss how to achieve end-to-end message exchanges by extending the proposed approach. The proposed scheme moves the mutual authentication phase from mobile nodes to their super nodes for fast and reliable implementation. Computer simulation results demonstrate that 1) the proposed schemes achieve better utilization of the network resources by limiting unauthorized traffic, 2)

the symmetric key based scheme outperforms the asymmetric key based scheme in terms of intermediate node computing power saving, and 3) the dominating set based routing outperforms the epidemic routing under the proposed information security scheme, in terms of the required number of forwarded messages, at the cost of increased number of lost messages and a slightly increased number of asymmetric key cryptographic operations.

Chapter 7

Conclusion and Further Research

7.1 Conclusion

The objective of this research is to achieve end-to-end information delivery over virtually continuous connectivity to roaming users with intermittent radio links over heterogeneous terrestrial wireless access networks. Regular network protocols fail to provide successful communications due to users' frequent disconnections and long disconnection periods. We propose a system architecture that is based on the store-and-forward message delivery strategy used in a DTN, using the idea of super nodes. A super node traces the location of a roaming user and acts as the user's delegate when the user is unavailable. Routing over the super node architecture is a real challenge for networks with no infrastructure such as mobile ad-hoc networks. We propose a new routing technique for mobile ad-hoc networks. This technique introduces the new concept of virtual network topology. We further propose the idea of analyzing node mobility model to better

estimate the contact probability. We extend the proposed routing technique by employing the mobility model analysis results to achieve better performance. Due to inability to control message routes over the super node architecture, new security techniques should be considered to satisfy the system constraints. We introduce two security techniques to secure message exchanges and to control the network access. The accomplishments in this thesis are summarized as follows:

- *The super node architecture*: The problem of intermittent connections in wireless networks has been addressed in the literature. The store-and-forward technique is introduced for successful communications over challenged networks. We explore the DTN architecture for application over heterogeneous wireless networks to support user roaming. Then, we study the problem of routing over DTN networks, and overview the different routing efforts in this field and how they relate to our research problem. Based on the DTN architecture, the system model of the super node architecture is proposed as a solution for providing a virtual connectivity for users roaming over heterogeneous wireless networks. The super node approach is compared with other possible approaches also based on the DTN store-and-forward technique for message delivery. A simulation study is presented, which shows the effectiveness of the super node approach, in terms of, the number of undelivered messages and the total number of message exchanges. The super node approach outperforms the epidemic based approach, especially for networks with a large number of nodes.

- *Dominating set based routing*: In Chapter 4, we focus on routing for networks that have no infrastructures such as MANETs. The new concept of virtual network topology for a DTN is proposed. The virtual topology

is argued to be a better representation of DTN based networks. Unlike the traditional network topology that represents the current physical connections among nodes, the virtual topology represents the probabilities of future connections (*i.e.*, contacts) among nodes. Based on the virtual network topology, a new routing technique is proposed. The routing technique is based on calculating a connected dominating set for the virtual network topology. We propose a new greedy algorithm to calculate the dominating set for the virtual topology. A new technique is presented to estimate the probability of future contacts based on the duration of previous contacts among nodes. The simulation study shows that the proposed dominating set routing is more efficient than the epidemic routing in terms of network resource utilization, and that using the contact duration to estimate the probability of future contacts is more effective than using the number of previous contacts.

- *Node mobility analysis and improved routing*: To further enhance the system performance, in Chapter 5, we propose to employ the node mobility model to better estimate the probability of contacts. A detailed analysis of the proposed node mobility model is presented, which finds the distribution of node inter-meeting times. Based on the distribution, we propose a new algorithm for dominating set calculation that can improve the system performance by reducing the size of the selected dominating set. The simulation study demonstrates how the newly proposed algorithm performs in comparison with other algorithms. Moreover, the idea of randomly selecting the dominating set for the virtual topology is discussed. It is shown that the random selection technique gives very poor results in comparison with the other proposed techniques. This shows

that reducing the dominating set size only does not improve the system performance if the dominating set members are not selected accurately.

- *Preventing unauthorized messages and achieving end-to-end message security*: In Chapter 6, we address some security challenges within the super node system. We focus on the problem of unauthorized network resource usage for a network with no infrastructure within the super node system. We propose to adapt PKI certificate to solve this problem and discuss the pros and cons of using this solution. Further, we introduce the new idea of separating message legitimate check problem from the message sender authentication problem. Our new technique uses the concept of one-way key chain to address this problem. We further introduces the challenges to provide secure end-to-end message exchange over the super node system. Our new solution uses symmetric key cryptography to reduce the computational overhead introduced by asymmetric key cryptography techniques. A simulation study is conducted that demonstrate how effective the proposed technique and how these techniques perform under the different employed DTN routing techniques

7.2 Further Research

In this thesis, we have studied some key research issues related to achieving virtualy continuous connectivity for roaming users over heterogeneous wireless networks. Our results demonstrate the effectiveness of our proposed approaches, however our investigations also reveal other important research directions to further improve the proposed system performance. This research can be extended in several directions, as addressed in the following:

- *The super node system reliability*: During this research it is assumed that the super nodes are reliable in terms of computations and inter-communications. A very interesting challenge is how the system can tolerate the failure of one or more of the super nodes. Some techniques, such as node replication, should be applied to ensure system reliability.

- *System scalability and load balancing*: System scalability is another main concern that needs to be considered for actual implementation of the proposed system. The proposed system should support thousands of users while maintaining acceptable quality of service for each user. In Chapter 3 we present the custody transfer as a solution to achieve load balancing among super nodes and reduce the communications cost; however this needs to be further investigated under specific system design constraints.

- *Buffer management*: The buffer management in the routing techniques studied in this thesis employs a simple scheme of removing the oldest message in case of overflow. Many recent studies such as [134, 135] address the problem of buffer management strategies for the DTNs. The proposed routing scheme should be studied under other more intelligent buffer management schemes for better performance.

- *PKI lightweight certificates*: Using lightweight certificates to improve the super node system security is a subject that needs further investigation. Using the ECQV implicit certificate scheme introduced in Section 6.6.2 instead of the regular certificate is a promising direction of research that needs to be further investigated.

- *The dominating set based routing*: The proposed routing technique is mainly considered for MANETs that are part of the super node system.

Applying the technique to other types of DTNs is an interesting topic, for example, to a MANET without a DTN gateway. A distributed algorithm for calculating the dominating set should be developed based on system constraints. Moreover, without the existence of a gateway and with node frequent connections/disconnections, a method is needed to dynamically maintain the dominating set. Dynamically maintaining the calculated dominating set is still an open issue for research.

Bibliography

[1] H. Samuel, W. Zhuang, and B. Preiss, "Improving The Dominating-Set Routing over Delay Tolerant Mobile Ad-hoc Networks Via Estimating Node Intermeeting Times," *EURASIP Journal on Wireless Communications and Networking, Special issue on Opportunistic and Delay Tolerant Networks*, Vol. 2011, Article ID 402989, 2011.

[2] H. Samuel, W. Zhuang, and B. Preiss, "Improving Dominating Set Routing Performance Via Node Mobility Model," in *Proc. IEEE Globecom'10*, November 2010.

[3] H. Samuel and W. Zhuang, "Preventing unauthorized messages and achieving end-to-end security in delay tolerant heterogeneous wireless networks," *Journal of Communications, Special Issue on Delay Tolerant Networks, Architecture, and Applications*, vol. 5, no. 2, 2010.

[4] H. Samuel and W. Zhuang,"Preventing unauthorized messages in DTN based mobile ad hoc networks," in *Proc. IEEE Globecom'09*, November 2009.

[5] H. Samuel, W. Zhuang, and B. Preiss, "DTN based dominating set routing for MANET in heterogeneous wireless networking," *Mobile Networks and Applications*, vol. 14, pp. 154 – 164, April 2009.

[6] H. Samuel, W. Zhuang, and B. Preiss, "DTN based dominating set routing technique for mobile ad hoc networks," in *Proc. QShine'08*, July 2008.

[7] H. Samuel, W. Zhuang, and B. Preiss, "Routing over interconnected heterogeneous wireless networks with intermittent connections," in *Proc. IEEE ICC'08*, pp. 2282 – 2286, May 2008.

[8] N. Santos, L. Veiga, and P. Ferreira, "Transaction policies for mobile networks," in *Proc, IEEE Intern. Workshop on Policies for Distributed Systems and Networks 2004*, pp. 55–64, 7-9 June 2004.

[9] N. Santos and P. Ferreira, "Making distributed transactions resilient to intermittent network connections," in *Proc. IEEE WOWMOM'06*, pp. 598–602, 2006.

[10] D. Dwyer and V. Bharghavan, "A mobility-aware file system for partially connected operation," *ACM SIGOPS Operating Systems Review*, vol. 31, no. 1, pp. 24–30, Jan. 1997.

[11] A. Balasubramanian, Y. Zhou, W. B. Croft, B. N. Levine, and A. Venkataramani, "Web search from a bus," in *Proc. ACM CHANTS'07*, pp. 59–66,2007.

[12] I. Akyildiz, J. Xie, and S. Mohanty, "A survey of mobility management in next-generation all-IP-based wireless systems," *IEEE Wireless Communications* , vol. 11, no. 4, pp. 16–28, Aug. 2004.

[13] A. Misra, S. Das, A. Dutta, A. McAuley, and S. Das, "IDMP-based fast handoffs and paging in IP-based 4G mobile networks," *IEEE Communications Magazine*, vol. 40, no. 3, pp. 138–145, Mar 2002.

[14] C. Perkins, "IP mobility support for IPv4," *RFC3344*, Jan 2002.

[15] A. Campbell, J. Gomez, S. Kim, A. Valko, C.-Y. Wan, and Z. Turanyi, "Design, implementation, and evaluation of cellular IP," *IEEE Personal Communications*, vol. 7, no. 4, pp. 42–49, Aug 2000.

[16] R. Ramjee, K. Varadhan, L. Salgarelli, S. Thuel, S.-Y. Wang, and T. La Porta, "HAWAII: a domain-based approach for supporting mobility in wide-area wireless networks," *IEEE/ACM Transactions on Networking*, vol. 10, no. 3, pp. 396–410, Jun 2002.

[17] I. Akyildiz and W. Wang, "A dynamic location management scheme for next-generation multitier pcs systems," *IEEE Transactions on Wireless Communications*, vol. 1, no. 1, pp. 178–189, Jan 2002.

[18] M. Shi, H. Rutagemwa, X. Shen, J. Mark, and A. Saleh, "A service-agent-based roaming architecture for WLAN/Cellular integrated networks," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 5, pp. 3168–3181, Sept. 2007.

[19] M. Buddhikot, G. Chandranmenon, S. Han, Y. Lee, S. Miller, and L. Salgarelli,"Integration of 802.11 and third-generation wireless data networks," in *Proc. IEEE INFOCOM'03*, vol. 1, pp. 503–512 vol.1, 30 March–3 April 2003.

[20] R. Hsieh, Z. Zhou, and A. Seneviratne, "S-MIP: a seamless handoff architecture for mobile IP,"in *Proc. IEEE INFOCOM'03*, vol. 3, pp. 1774–1784 vol.3, 30 March–3 April 2003.

[21] H. Yokota, A. Idoue, T. Hasegawa, and T. Kato, "Link layer assisted mobile IP fast handoff method over wireless LAN networks," in *Proc. ACM MobiCom'02*, pp. 131–139, 2002.

[22] H. Rutagemwa, S. Pack, X. Shen, and J. Mark, "Robust cross-layer design of wireless profiled TCP mobile receiver for vertical handover," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3899–3911, Nov. 2007.

[23] M. E. Kounavis, A. T. Campbell, G. Ito, and G. Bianchi, "Design, implementation, and evaluation of programmable handoff in mobile networks," *Mobile Networks and Applications*, vol. 6, no. 5, pp. 443–461, 2001.

[24] "Delay tolerant network research group, http://www.dtnrg.org/." [Online]. Available: http://www.dtnrg.org/

[25] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proc/ ACM SIGCOMM '03*, pp. 27–34, 2003.

[26] R. Nichols, A. Hammons, D. Tebben, and A. Dwivedi, "Delay tolerant networking for free-space optical communication systems," in *Proc. IEEE Sarnoff Symposium 2007*, pp. 1–5, April 2007.

[27] G. Papastergiou, I. Psaras, and V. Tsaoussidis, "Deep-space transport protocol: A novel transport scheme for space DTNs," *Computer Communications*, vol. 32, no. 16, pp. 1757–1767, Oct. 2009.

[28] S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst, K. Scott, and H. Weiss, "Delay-tolerant networking: an approach to interplanetary internet," *IEEE Communications Magazine*, vol. 41, no. 6, pp. 128–136, June 2003.

[29] J.-H. Cui, J. Kong, M. Gerla, and S. Zhou, "The challenges of building mobile underwater wireless networks for aquatic applications," *IEEE Network - Special Issue Wireless Sensor Networks*, vol. 20, no. 3, pp. 12–18, May. 2006.

[30] A. Mahdy, "A perspective on marine wireless sensor networks," *Journal of Computing Sciences in Colleges*, vol. 23, no. 6, pp. 89–96, 2008.

[31] J. Partan, J. Kurose, and B. N. Levine, "A survey of practical issues in underwater networks," in *Proc. ACM WUWNet'06*, pp. 17–24, 2006.

[32] C. E. Perkins ,and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. IEEE WMCSA '99*, pp. 90–100, 1999.

[33] R. Morris, J. Jannotti, F. Kaashoek, J. Li, and D. Decouto, "CarNet: a scalable ad hoc wireless network system," in *Proc. ACM EW SIGOPS European workshop*, pp. 61–65, 2000.

[34] E. Perevalov and R. Blum, "Delay limited capacity of ad hoc networks: Asymptotically optimal transmission and relaying strategy," in *Proc. IEEE INFOCOM'03*, vol. 2, pp. 1575–1582, 30 March–3 April 2003.

[35] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, vol. 353, pp. 153–181, 1996.

[36] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, and D. Rubenstein,"Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with zebranet," in *Proc. ACM ASPLOS-X'02*, Vol. 37, No. 10, pp. 96–107, Oct. 2002.

[37] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proc. ACM MobiCom'00*, pp. 243–254, 2000.

[38] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proc. ACM SIGCOMM'94*, pp. 234–244, 1994.

[39] D. Nain, N. Petigara, and H. Balakrishnan, "Integrated routing and storage for messaging applications in mobile ad hoc networks," *Mobile Networks and Applications*, vol. 9, no. 6, pp. 595–604, 2004.

[40] Y.-B. Ko and N. H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks," in *Proc. ACM/IEEE MobiCom'98*, pp. 66–75, 1998.

[41] Q. Li and D. Rus, "Sending messages to mobile users in disconnected ad-hoc wireless networks," in *Proc. ACM MobiCom'00*, pp. 44–55, 2000.

[42] J. A. Davis, A. H. Fagg, and B. N. Levine, "Wearable computers as packet transport mechanisms in highly-partitioned ad-hoc networks," in *Proc. IEEE ISWC'01*, pp. 141–148, 2001.

[43] A. Doria, M. Uden, and D. P. Pandey, "Providing connectivity to the saami nomadic community," in *Proc. 2nd Int. Conf. on Open Collaborative Design for Sustainable Development, Bangalore, India*, December 2002.

[44] W. Zhao, M. Ammar, and E. Zegura, "A message ferrying approach for data delivery in sparse mobile ad hoc networks," in *Proc. ACM MobiHoc'04*, pp. 187–198, 2004.

[45] R. Shah, S. Roy, S. Jain, and W. Brunette, "Data MULEs: Modeling a three-tier architecture for sparse sensor networks," in *Proc. IEEE SNPA'03*, pp. 30–41, 2003.

[46] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, pp. 102 – 114, Aug 2002.

[47] Y. Yang, H. Wu, and W. Zhuang, "Mester: minimum energy spanning tree for efficient routing in wireless sensor networks," in *Proc. QShine'06*, Aug. 2006, .

[48] B. Pasztor, M. Musolesi, and C. Mascolo, "Opportunistic mobile sensor data collection with scar," in *Proc. IEEE MASS'07*, pp. 1 – 12, Oct. 2007 .

[49] M. M. H. Khan, L. Luo, C. Huang, and T. Abdelzaher, "SNTS: sensor network troubleshooting suite," in *Proc. IEEE DCOSS'07*, pp. 142–157, 2007.

[50] A. Boulis, C.-C. Han, and M. B. Srivastava, "Design and implementation of a framework for efficient and programmable sensor networks," in *Proc. ACM MobiSys'03*, pp. 187–200, 2003.

[51] C. Srisathapornphat, C. Jaikaeo, and C.-C. Shen, "Sensor information networking architecture," in *Proc. IEEE ICPP'00*, pp. 23 – 30, 2000.

[52] D. Borsetti, C. Casetti, C.-F. Chiasserini, M. Fiore, and J. M. Barceló-Ordinas, "Virtual data mules for data collection in road-side sensor networks," in *Proc. ACM MobiOpp'10*, pp. 32–40, 2010.

[53] R. Lu, X. Lin, H. Zhu, and X. Shen, "Security in service-oriented vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 6, pp. 2772 – 2785, Apr. 2010.

[54] H. Zhu, R. Lu, X. Lin, and X. Shen, "Security in service-oriented vehicular networks," *IEEE Wireless Communications, Special Issue on Service Oriented Broadband Wireless Network Architecture,*, vol. 16, no. 4, pp. 16 – 22, Aug. 2009.

[55] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM'08*, pp. 1229 – 1237, Apr. 2008.

[56] W. Zhao and M. H. Ammar, "Message ferrying: Proactive routing in highly-partitioned wireless ad hoc networks," in *Proc. IEEE FTDCS'03*, pp. 308–314, May 2003.

[57] J. LeBrun, C.-N. Chuah, D. Ghosal, and M. Zhang, "Knowledge-based opportunistic forwarding in vehicular wireless ad hoc networks," in *Proc. IEEE VTC'05*, vol. 4, 2005, pp. 2289– 2293.

[58] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," April 2000. [Online]. Available: citeseer.ist.psu.edu/vahdat00epidemic.html

[59] A. Jindal and K. Psounis, "Performance analysis of epidemic routing under contention," in *Proc. ACM IWCMC'06*, pp. 539–544, 2006.

[60] X. Zhang, G. Neglia, J. Kurose, and D. Towsley, "Performance modeling of epidemic routing," *Computer Networks*, vol. 51, no. 10, pp. 2867–2891, 2007.

[61] R. Ramanathan, R. Hansen, P. Basu, R. Rosales-Hain, and R. Krishnan, "Prioritized epidemic routing for opportunistic networks," in *Proc. ACM MobiOpp'07*, pp. 62–66, 2007.

[62] I. F. Akyildiz, Özgür B. Akan, C. Chen, J. Fang, and W. Su,"Interplanetary internet: state-of-the-art and research challenges," *Computer. Networks*, vol. 43, no. 2, pp. 75–112, 2003.

[63] S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," in *Proc. ACM SIGCOMM'04*, pp. 145–158, 2004.

[64] P. Mundur, S. Lee, and M. Seligman, "Routing in intermittent network topologies," in *Proc. ACM MSWiM'06*, pp. 385–389, 2006.

[65] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," *ACM SIGMOBILE Mobile Computing and Communications Review* , vol. 7, no. 3, pp. 19–20, 2003.

[66] X. Chen and A. L. Murphy, "Enabling disconnected transitive communication in mobile ad hoc networks," in *Proc. of Workshop on Principles of Mobile Computing, colocated with PODC01*, pp. 21–23, 2001.

[67] J. Ghosh, H. Q. Ngo, and C. Qiao, "Mobility profile based routing within intermittently connected mobile ad hoc networks (ICMAN)," in *Proc. ACM IWCMC'06*, pp. 551–556, 2006.

[68] J. Leguay, T. Friedman, and V. Conan, "DTN routing in a mobility pattern space," in *Proc. ACM WDTN'05*, pp. 276–283, 2005.

[69] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "MaxProp: Routing for vehicle-based disruption-tolerant networks," in *Proc. IEEE INFOCOM'06*, pp. 1 – 11, 2006.

[70] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *Proc. ACM WDTN'05*, pp. 252–259, 2005.

[71] P. Hui, J. Crowcroft, and E. Yoneki, "BUBBLE Rap: social-based forwarding in delay tolerant networks," in *Proc. ACM MobiHoc'08*, pp. 241–250, 2008.

[72] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Efficient routing in intermittently connected mobile networks: the single-copy case," *IEEE/ACM Transactions on Networking*, vol. 16, no. 1, pp. 63–76, 2008.

[73] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Efficient routing in intermittently connected mobile networks: the multiple-copy case," *IEEE/ACM Transactions on Networking*, vol. 16, no. 1, pp. 77–90, 2008.

[74] E. Bulut, Z. Wang, B. K. Szymanski, "Time dependent message spraying for routing in intermittently connected networks," in *Proc. IEEE Globecom'08*, Nov. 2008.

[75] E. Bulut, Z. Wang, and B. K. Szymanski, "Impact of social networks on delay tolerant routing," in *Proc. IEEE GLOBECOM'09*, pp. 1804–1809 , 2009.

[76] L. Tang, Q. Zheng, J. Liu, and X. Hong, "Selective message forwarding in delay tolerant networks," *Mobile Networks and Applications*, vol. 14, no. 4, pp. 387–400, 2009.

[77] H. Jiang, W. Zhuang, and X. Shen, "Cross-layer design for resource allocation in 3G wireless networks and beyond," *IEEE Communications Magazine*, vol. 43, no. 12, pp. 20–126, Dec. 2005.

[78] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker, "A scalable content-addressable network," in *Proc. ACM SIGCOMM'01*, pp. 161–172, 2001.

[79] J.-P. Hubaux, T. Gross, J.-Y. Le Boudec, and M. Vetterli, "Toward self-organized mobile ad hoc networks: the terminodes project," *IEEE Communications Magazine*, vol. 39, no. 1, pp. 118–124, Jan 2001.

[80] V. Lo, D. Zhou, Y. Liu, C. GauthierDickey, and J. Li, "Scalable supernode selection in peer-to-peer overlay networks," in *Proc. IEEE HOT-P2P'05* , pp. 18–25, July 2005.

[81] H. A. Samuel, Y. H. Dakroury, and H. I. Shahein, "Recard: Using recommendation cards approach for building trust in peer-to-peer networks," in *Proc. of ISPEC'05*, LNCS, vol. 3439, pp. 280–292, 2005.

[82] Y. Y. Zhang and Y. Y. Fang, "A fine-grained reputation system for reliable service selection in peer-to-peer networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 8, pp. 1134 – 1145, Aug. 2007.

[83] G. Huang, S. Hu, and J. Jiang, "Scalable reputation management with trustworthy user selection for p2p MMOGs," *Intern. Journal of Advanced Media and Communication*, vol. 2, no. 4, pp. 380–401, 2008.

[84] E. Damiani, D. C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante,"A reputation-based approach for choosing reliable resources in peer-to-peer networks," in *Proc. ACM CCS'02*, pp. 207–216, 2002.

[85] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. ACM MobiCom'00*, pp. 255–265, 2000.

[86] H. Janzadeh, K. Fayazbakhsh, M. Dehghan, and M. S. Fallah, "A secure credit-based cooperation stimulating mechanism for MANETs using hash chains," *Future Generation Computer Systems*, vol. 25, no. 8, pp. 926–934, 2009.

[87] S. Z. Yale and S. Zhong, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Proc. IEEE INFOCOM'03*, pp. 1987–1997, 2003.

[88] A. I. T. Rowstron and P. Druschel, "Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems," in *Proc. IFIP/ACM Middleware'01*, pp. 329–350, 2001.

[89] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," in *Proc. ACM SIGCOMM'01*, pp. 149–160, 2001.

[90] J. Wu, M. Gao, and I. Stojmenovic, "On calculating power-aware connected dominating sets for efficient routing in ad hoc wireless networks," in *Proc. IEEE Int. Conf. on Parallel Processing*, pp. 346–354, 3–7 Sept. 2001.

[91] H. Dang and H. Wu, "Mobility models for delay-tolerant mobile networks," in *Proc. IEEE third Int. Conf. on Sensor Technologies and Applications*, pp. 55–60, 2009.

[92] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, "Impact of human mobility on opportunistic forwarding algorithms," *IEEE Transactions on Mobile Computing*, vol. 6, no. 6, pp. 606–620, 2007.

[93] P. Luo, H. Huang, W. Shu, M. Li, and M.-Y. Wu, "Performance evaluation of vehicular DTN routing under realistic mobility models," in *Proc. IEEE WCNC'08*, pp. 2206–2211, 2008 .

[94] H. Zhu, L. Fu, G. Xue, Y. Zhu, M. Li, and L. M. Ni, "Recognizing exponential inter-contact time in VANETs," in *Proc. IEEE INFOCOM'10*, pp. 101–105, 2010.

[95] H. Zhu, M. Li, Y. Zhu, and L. M. Ni, "HERO: Online real-time vehicle tracking," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, pp. 740–752, 2009.

[96] H. Cai and D. Y. Eun, "Toward stochastic anatomy of inter-meeting time distribution under general mobility models," in *Proc. ACM MobiHoc'08*, pp. 273–282, 2008.

[97] X. Li and X. Zhou, "Bounded-delay, probability-based routing in intermittently connected mobile ad hoc networks," in *Proc. of IEEE ICDCS08*, pp. 210–215, 2008.

[98] L. Ruan, H. Du, X. Jia, W. Wu, Y. Li, and K.-I. Ko, "A greedy approximation for minimum connected dominating sets," *Theoretical Computer Science*, vol. 329, no. 1–3, pp. 325 – 330, 2004.

[99] Y. Li, M. T. Thai, F. Wang, C.-W. Yi, P.-J. Wan, and D.-Z. Du, "On greedy construction of connected dominating sets in wireless networks: Research articles," *Wireless Communications and Mobile Computing*, vol. 5, no. 8, pp. 927–932, 2005.

[100] K. Tan, Q. Zhang, and W. Zhu, "Shortest path routing in partially connected ad hoc networks," in *Proc. IEEE Globecom'03*, vol. 2, December 2003, pp. 1038 – 1042.

[101] K. Fall and S. Farrell, "DTN: an architectural retrospective," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 5, pp. 828–836, June 2008.

[102] S. Farrell, S. Symington, H. Weiss, and P. Lovell, "Delay-tolerant networking security overview," *IRTF, DTN research group*, February 2008.

[103] Q. He, D. Wu, and P. Khosla, "SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks," in *Proc. IEEE WCNC'04*, pp. 825 – 830, 2004.

[104] H. Zhu, X. Lin, R. Lu, and X. Shen, "BBA: An efficient batch bundle authentication scheme for delay tolerant networks," in *Proc. ChinaCom'08*, pp. 23 – 28, 2008.

[105] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A secure multilayer credit-based incentive scheme for delay-tolerant networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 4628 – 4639, 2009.

[106] R. Lu, X. Lin, H. Zhu, X. Shen, and B. Preiss, "Pi: a practical incentive protocol for delay tolerant networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1483–1493, 2010.

[107] K. Ren, W. Lou, and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks," in *Proc. IEEE SECON'07*, pp. 223–232, June 2007.

[108] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[109] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM'08*, pp. 1229–1237, April 2008.

[110] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. INFOCOM'08*, pp. 246–250, April 2008.

[111] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[112] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. IEEE ICC'08*, pp. 1451–1457, May 2008.

[113] "Crypto++ library is a free c++ class library of cryptographic schemes," *Available at http://www.cryptopp.com/.*

[114] H. Zhu, "Security in delay tolerant networks," in *PhD thesis, University of Waterloo.*

[115] H. Zhu, X. Lin, R. Lu, X. Shen, D. Xing, and Z. Cao, "An opportunistic batch bundle authentication scheme for energy constrained dtns," in *Proc. IEEE INFOCOM' 10*, pp. 605–613, 2010.

[116] E. Barker, "Suite B cryptography," *NIST Computer Security Division - Computer Security Resource Center, Technical meeting presentation, available at http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2006-03E%5FBarker-March2006-ISPAB.pdf*, March 22, 2006.

[117] N. S. Agency, "NSA suite B cryptography," http://www.nsa.gov/ia/programs /suiteb%5Fcryptography/.

[118] N. Asokan, K. Kostiainen, P. Ginzboorg, J. Ott, and C. Luo, "Applicability of identity-based cryptography for disruption-tolerant networking," in *Proc. ACM MobiOpp'07*, pp. 52–56, 2007.

[119] H. Zhu, X. Lin, R. Lu, X. Shen, and P.-H. Ho, "BBA: An efficient batch bundle authentication scheme for delay tolerant networks," in *Proc. IEEE GLOBECOM'08*, pp. 1–5, 2008.

[120] J. Burgess, G. D. Bissias, M. D. Corner, and B. N. Levine, "Surviving attacks on disruption-tolerant networks without authentication," in *Proc. ACM MobiHoc'07*, pp. 61–70, 2007.

[121] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," RFC 3280, April 2002.

[122] A. Perrig, R. Canetti, D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," 2002. [Online]. Available: citeseer.ist.psu.edu/perrig02tesla.html

[123] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proc. ACM CRYPTO'01*, pp. 213–229, 2001.

[124] A. Seth and S. Keshav, "Practical security for disconnected nodes," in *Proc. IEEE NPSec'05*, pp. 31–36, Nov. 2005.

[125] J.-P. Hubaux, L. Buttyán, and S. Capkun, "The quest for security in mobile ad hoc networks," in *Proc. ACM MobiHoc'01*, pp. 146–155, 2001.

[126] H. Labiod, H. Afifi, and C. de Santis, *Wi-Fi ^{TM}, Bluetooth^{TM}, Zigbee^{TM}and WiMax^{TM}*. P.O. Box 17, 3300 AA Dordrecht, The Netherlands.: Springer, 2007.

[127] "The zigbee alliance, http://www.zigbee.org." [Online]. Available: http://www.zigbee.org

[128] M. Bohge and W. Trappe, "Tesla certificates: An authentication tool for networks of compute-constrained devices," in *In Proc. of WPMC 03*, 2003.

[129] M. Bohge and W. Trappe, "An authentication framework for hierarchical ad hoc sensor networks," in *In Proc. of ACM WiSE03*, 2003.

[130] A. Roy-Chowdhury and J. Baras, "A lightweight certificate-based source authentication protocol for group communications in hybrid wireless/satellite networks," in *In Proc. of IEEE GLOBECOM'08*, pp. 1 – 6, 2008.

[131] Y. Lee, J. Lee, C. Chung, and J. Song, "Design and analysis of a lightweight certificate revocation mechanism for VANET," in *in Proc. of IEEE ICCE '06*, pp. 103 – 104, Jan 2006.

[132] J. J. Haas., Y.-C. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET," in *in Proc. of ACM VANET '09*, pp. 89–98, 2009.

[133] S. f. e. c. Certicom Research, "Sec 4: Elliptic curve cryptography," *Draft document, Version 0.91* , Available at http://www.secg.org/download/aid-775/sec4-ECQV-v091.pdf, 2008.

[134] A. Krifa, C. Barakat, and T. Spyropoulos, "Optimal buffer management policies for delay tolerant networks," in *in Proc. of IEEE SECON'08*, 2008, pp. 260 – 268.

[135] Y. Li, M. Qian, D. Jin, L. Su, and L. Zeng, "Adaptive optimal buffer management policies for realistic DTN," in *Proc. IEEE GLOBECOM'09*, pp. 2683–2687 , 2009.

[136] S. M. Ross, *Introduction to Probability Models, Ninth Edition.* Orlando, FL, USA: Academic Press, Inc., 2006.

Appendix A

Poisson Process

This appendix discuss some definitions and properties of Poisson process [136] that are used to prove the theorems proposed in Chapter 5.

Definition A.1. *A function f(.) is said to be o(h) if*

$$\lim_{h \to 0} \frac{f(h)}{h} = 0$$

Definition A.2. *A counting process* $\{N(t), t \geq 0\}$ *is a Poisson process with rate* λ, $\lambda > 0$ *if*

1. *N(0)=0.*
2. *The process has stationary and independent increments.*
3. $P\{N(h) = 1\} = \lambda h + o(h)$.
4. $P\{N(h) \geq 2\} = o(h)$.

A.1 Interarrival Time Distribution

Consider a poisson process $\{N(t), t \geq 0\}$, and let T_1 denote the time of the first event. For $n > 1$, let T_n denotes the time elapsed between the $(n-1)$ event and

the n event. The interarrival times is denoted by the sequence $\{T_n, n = 1, 2, \ldots\}$.

Proposition A.1. *The interarrival times* $\{T_n, n = 1, 2, \ldots\}$ *for a poisson process* $\{N(t), t \geq 0\}$ *with rate* λ *are iid exponential random variables with mean* $\frac{1}{\lambda}$

Proof. The first event occurs at time $\{T_1 > t\}$ if and only if no events occurs in the interval $[0, t]$, thus

$$P\{T_1 > t\} = P\{N(t) = 0\} = \exp^{-\lambda t} \frac{(\lambda t)^0}{0!} = \exp^{-\lambda t}$$

Hence, T_1 has an exponential distribution with mean $\frac{1}{\lambda}$.
For T_2:

$$P\{T_2 > t\} = E[P\{T_2 > t \mid T1\}]$$

However, for a Poisson process we have independent and stationary increments (by *Definition* A.2), then:

$$P\{T_2 > t \mid T_1 = h\} = P\{0 \text{ events in } (h, h + t] \mid T_1 = h\} = \exp^{-\lambda t}$$

Then, T_2 has an exponential distribution with mean $\frac{1}{\lambda}$ that is independent of T_1. Similarly, it can be proven for any $\{T_n, n > 1\}$. □

A.2 Classification of Poisson Arrivals

Considering a Poisson process $\{N(t), t \geq 0\}$ with rate λ, assume each time an event occurs it is considered of type x with probability p ,and of type y with probability $1 - p$ independently of all other events. Let $N_x(t)$ and $N_y(t)$ denote the number of type x and type y events occurring in $[0, t]$. The total number of events at any instance t is $N(t) = N_x(t) + N_y(t)$.

Proposition A.2. *$\{N_x(t), t \geq 0\}$ and $\{N_y(t), t \geq 0\}$ are Poisson processes with rates λp and $\lambda(1-p)$ respectively. Moreover, $\{N_x(t), t \geq 0\}$ and $\{N_y(t), t \geq 0\}$ are independent.*

Proof. To prove that proposition we need to prove that $N_x(t)$ and $N_y(t)$ satisfies *Definition* A.2. Considering $N_x(t)$ and *Definition* A.2 :

1. As $N(0) = 0$ then $N_x(0) = 0$.

2. $\{N_x(t), t \geq 0\}$ inherts the stationary and independent increment proerties of the process $\{N(t), t \geq 0\}$.

3. $P\{N_x(h) = 1\} = P\{N_x(h) = 1 \mid N(h) = 1\}P\{N(h) = 1\}$
   $+ P\{N_x(h) = 1 \mid N(h) \geq 2\}P\{N(h) \geq 2\}$
   $P\{N_x(h) = 1\} = p(\lambda h + o(h)) + o(h) = \lambda p h + o(h)$

4. $P\{N_x(h) \geq 2\} \leq P\{N(h) \geq 2\} = o(h)$

It is clear that $\{N_x(t), t \geq 0\}$ satisfies *Definition* A.2. As a result, $\{N_x(t), t \geq 0\}$ is a Poisson process with rate λp. A similar argument for $\{N_y(t), t \geq 0\}$ will show that it is a Poisson process with rate $\lambda(1-p)$. the probability of type x event in the interval $(t, t+h)$ is independent of all that occurs in intervals that do not overlap with this interval, so it is independent of knowledge of when type y event occurs. As a result, the two processes $\{N_x(t), t \geq 0\}$ and $\{N_y(t), t \geq 0\}$ are independent. □

Appendix B

Simulation Overview

In our simulation experiments, we use a discrete event simulator written in visual C sharp and MATLAB. In this section, we give a detailed overview of the simulation details.

At the initialization phase of a simulation, the number of nodes and the buffer size of each node are specified by the simulation parameters. In simulating the super node scheme, a number of super nodes is generated based on the number of super nodes parameter. Nodes are assigned statically to the super nodes, such as all the super nodes are assigned the same number of nodes (*e.g.*, in case of 100 nodes and 4 super nodes, super node with ID 1 is assigned nodes with ID $1 - 25$). At the end of the initialization phase, all nodes are associated randomly with the available networks.

For each node, a sequence of events in the simulation duration is generated randomly as follows. The events are connection, disconnection and movement events. The connection event specifies a random network ID to connect to and a network residence duration (generated as an exponential random variable with mean equal to the network mean residence time parameter). For simplicity, all

nodes have the same network mean residence time in all the networks. As the network residence duration expires, a disconnection event or a movement event will occur. In the case of a disconnection event, the disconnection duration is generated as an exponential random variable with mean equal to the disconnection mean time parameter. After the disconnection duration, a connection event is generated where the node reconnects to its previous network or to a new network with probabilities specified in the simulation parameters. In the case of a movement event, the node connects through a new network for a duration that is generated as an exponential random variable with a mean equal to the mean network residence time parameter.

As the simulation starts, message generation is done at every simulation step. Each connected node generates a new message with probability 0.5 and it chooses the message destination randomly. All messages are assigned the same time to live (*i.e.*, TTL) in units of simulation steps, which is specified by the TTL parameter. A message is sent over the network where the source node resides. If the node is connected to a WLAN or a cellular network, the message is delivered to the network gateway directly. In the case of a MANET, the message is forwarded to all nodes connected to the source node and stored at their local buffers. The message is forwarded at later simulation steps to other nodes until it reaches the gateway. When the message reaches the gateway, the message is forwarded to the destination super node (for the super node scheme) or forwarded to all attached gateways (in epidemic routing scheme). The super node forwards the message to the gateway of the network where the destination node resides. The gateway delivers the message to the destination directly, in the case of a WLAN or a cellular network, or to the nodes connected to the gateway in the case of a MANET.

The MANET network coverage is simulated as a square area divided into

square partitions, the number of partitions is specified in the simulation parameters. A node moves according to the node speed parameter. Nodes within the same partition are connected and can exchange messages; however, there is no inter-partition communication. The network gateway is fixed at a partition randomly chosen in the simulation initialization phase and remains fixed for the simulation duration. The gateway, similar to other nodes, can exchange messages only with nodes within its partition. Every node connected to the MANET makes a random movement over the network coverage partitions with a speed equal to the node speed parameter.

The MAC layer is assumed to be ideal. The number of messages that can be transferred per simulation step is specified by the simulation parameters. In case of a disconnection occurring before completing all messages transfer, only a subset of the messages is transferred.

At each simulation step, nodes are processed in ascending order of their IDs. Each node updates its message buffer by decrementing messages TTL field and by discarding any expired messages (whose TTL=0). A daemon thread examines a global buffer where references to all generated messages are stored in it, wherever a message is expired, it checks if its destination reported the reception of this message or not. If an expired message is not marked as received, it is marked as lost (*i.e.*, undelivered). Counters are updated to reflect the number of received and undelivered messages. Statistics are collected and logged to a specific log file, for every predefined number of simulation steps that is determined by a simulation parameter.