1-1-2013

An Energy Aware Trust Based Multipath Routing Scheme For Mobile Ad Hoc Networks

Michael Ryan Sahai
Ryerson University

An Energy Aware Trust Based Multipath Routing Scheme For Mobile Ad Hoc Networks

by

Michael Ryan Sahai

B.Sc., Ryerson University, Toronto, Canada, 2009

A Thesis

Presented to Ryerson University

in partial fulfillment of the

requirements for the degree of

Master of Science

in the Program of Computer Science

Toronto, Ontario, Canada, 2013

Author's Declaration

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 authorize Ryerson University to lend this thesis to other institutions or individuals for the purpose of scholarly research

I further authorize Ryerson University to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

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

Abstract

An Energy Aware Trust Based Multipath Routing Scheme for Mobile Ad Hoc Networks

Master of Science
Computer Science
Ryerson University

Message security in multi-hop infrastructure-less networks such as Mobile Ad Hoc Networks has proven to be a challenging task. A number of trust-based secure routing protocols has recently been introduced comprising of the traditional route discovery phase and a data transmission phase. In the latter, the action of relaying the data from one mobile node to another relies on the peculiarity of the wireless transmission medium as well as the capability of the source nodes to keep their energy level at an acceptable and reasonable level, posing another concern which is that of energy efficiency.

This thesis proposes an Energy-Aware Trust Based Multi-path secured routing scheme (E-TBM) for MANETs, based on the dynamic source routing protocol (DSR). Results show that the E-TBM scheme outperforms the Trust Based Multi-path (TBM) secured routing scheme [1], chosen as a benchmark, in terms of energy consumption of the selected routing paths, number of dead nodes, trust compromise and route selection time, chosen as performance metrics.

Acknowledgement

My utmost gratitude goes to my supervisor, Dr. Isaac Woungang for accepting me as his Masters student and guiding me with patience and encouragement. He has been abundantly helpful and has assisted me in numerous ways. Without his continual support and thoughtful mentoring, this thesis would not be possible.

Moreover, my appreciation goes to Dr. Sanjay Kumar Dhurandher and my friends in our DABNEL lab who were there when I needed help. Their assistance throughout the course of the program helped me accomplish my goals and it was a privilege working with them.

I would also like to thank my thesis committee for reviewing my work and taking the time to provide me with feedback and helpful comments.

I would also like to thank the school for giving me time off while I recovered from my accident which could have potentially stopped me from completing my research and masters degree all together.

I wish to thank my dad Sydney Sahai, mother Soonardaye Sahai and my sister Michelle Sahai. Without their love, guidance and motivation, I would not have accomplished as much as I have thus far. I would also like to thank my girlfriend Fiona Alli for her ever continuing support and love.

Contents

1 Introduction **1**

1.1 Motivation 2

1.2 Research Problem 3

1.3 Approach 3

1.4 Thesis Contributions 4

1.5 Thesis Organization 4

2 Background And Related Work **5**

2.1 Background 5

2.1.1 Mobile Ad Hoc Networks 5

2.1.2 DSR Protocol 6

2.2 Energy-Efficiency as a Key Concern when Designing Multipath Routing for Wireless Ad hoc Networks 8

2.3 Approaches To Achieve Secure Energy-Efficient Routing in Wireless Ad Hoc Networks 9

2.3.1 Energy-Aware Routing Schemes for MANETs 9

2.3.2 Energy-Aware Secured Routing Schemes for MANETs 12

3 Methodology **17**

3.1 Enhanced Trust Based Multipath DSR Protocol With Soft Encryption Algorithm (E-TBM) 17

3.1.1 Message Encryption 18

3.1.2 Energy Aware Message Routing Using DSR 19

3.1.2.1 Trust Assignment Strategy 19

3.1.2.2 Energy-Aware Routing Mechanism 21

3.1.3 Message Decryption 27

4 Performance Evaluation **28**

4.1 Simulation Tool 28

4.2 Performance Metrics 29

4.3 Assumptions 30

4.4 Simulation Parameters 30

4.5 Simulation Scenario 31

4.6 Simulation Results 32

5 Conclusions **36**

Appendices **37**

Appendix A **38**

A.1 Overview of the GloMoSim System 38

A.2 Assumptions 39

A.3 Interface Requirements 39

A.3.1 Command Line Interface 39

A.3.2 Software Resource Requirements 39

Bibliography **51**

List of Figures

2.1 An example of a wireless network 6

2.2 An example of a MANET 6

2.3 Original RREP packet format 7

3.1 Basic Message sending between a source and destination node 18

3.2 Proposed Message Security Scheme 18

3.3 Assignment of Trust Values to Nodes 20

3.4 Illustrating the DSR protocol 25

3.5 RREP packet format 25

3.6 E-TBM routing scheme operations 26

4.1 Comparison of Trust Compromise 32

4.2 Route Selection time for E-TBM vs. TBM schemes 33

4.3 Total energy consumed in the selected routing paths for E-TBM vs. TBM schemes 34

4.4 Total energy consumed based on E-TBM vs. TBM schemes. 35

4.5 Number of dead nodes in the E-TBM vs. TBM schemes 35

List of Tables

4.1 Simulation Parameters 31

List of Algorithms

1 E-TBM 24

List of Abbreviations

ACK	Transmission Acknowledgement
AODV	Ad Hoc On-Demand Vector
CBR	Constant Bit Rate
DSR	Dynamic Source Routing
DSDV	Destination Sequenced Distance Vector Routing
E-TBM	Energy-aware Trust Based Multipath Routing Scheme
GloMoSim	Global Mobile Information System Simulator
MANETs	Mobile Ad Hoc Networks
OLSR	Optimized Link State Routing
RREP	Route Reply
RREQ	Route Request
RRER	Route Error
TCP	Transmission Control Protocol
TBM	Trust Based Multipath Routing Algorithm

Chapter 1

Introduction

A mobile ad-hoc network (MANET) is a collection of highly wireless mobile nodes organized to create a temporary connection between them to forward data, without any pre-established network infrastructure or extraneous hardware to assist in this communication. To fulfill this capacity, some form of collaborative or cooperative multi-hop strategy is required to exist between the mobile nodes, which may not necessary prevail since misbehaving nodes could be part of the current set of MANET nodes. Therefore, securing the message delivery in MANETs is a challenging task.

Typically, the routing mechanism involves two steps, namely the route discovery phase and the actual data transmission phase using the discovered secured routes. The former relies on the underlying targeted routing protocol (in this thesis, we use trust-based multi-path DSR). The latter involves investigating the peculiarities of the wireless transmission medium used, as well as determining the required battery level of the source nodes involved in the data transmission process. Indeed, when performing data transmission, it is essential that the nodes (here referred to as battery operated computing devices) that carry out the operation, be energy conserving so that their individual battery life can be prolonged, and the maximum lifetime of the network can be achieved. These facts have led to the consideration of energy-efficiency as another important design aspect that should be taken into account in the routing decision. The goal is to achieve secure routing while lowering the network's overall power consumption and number of dead nodes; where a dead node is defined as a node which has completely depleted its power level. When a node is drained of all its available power, it no longer plays a role in the route selection process.

This thesis adds energy considerations into a recently proposed message security scheme in MANETs (so-called Trust Based Multi-path message security (TBM)) [1], in order to strengthen its design. Typically, the route discovery and selection algorithm in [1] is substantially modified to take into consideration the energy level of the selected routing paths while maintaining their security and trust levels, resulting in our so-called Energy-Aware Trust Based Multi-path (E-TBM) message security scheme. The modification consists of assigning a power-aware metric [2] to each node involved in the selected routing paths so as to quantify the amount of energy consumed by the node, thereby determining the energy consumption necessary to maintain an acceptable level of message security in the network. The E-TBM approach consists of a combination of trust assignment mechanism, soft-encryption technique, and multi-path DSR-based routing, where the decision on the routing selection paths is energy constrained.

1.1 Motivation

Wireless networking has gained a lot of attention in recent years. Recent developments in the field have led us to focus our research on energy efficient secure mobile ad hoc networks. Integrity, confidentiality, and availability of data can only be assured if all the security issues have been addressed. Thus energy efficiency and secured routing schemes for MANETs have been some of the main areas of focus for the functionality of such networks.

In this thesis, we will address the techniques used to accomplish the balance of an energy efficient and secure network.

1.2 Research Problem

In MANETs, there lies a deficiency in the manner to which nodes communicate with each other. When a node in a MANET attempts to transmit data, the message could potentially be intercepted by malicious nodes, which could lead to the loss of message integrity. Nodes in a MANET are more than likely to be powered by battery power, and as a result, it is necessary to maintain the battery power of nodes so that the data can be sent and received. We seek a balance so that we can securely transmit the data between nodes in the network, while also taking into account the power required to transmit the data.

The goal of this thesis is to implement an energy-aware trust-based multiple path routing scheme based on an algorithm referred to as TBM [1] . We have modified the current route selection algorithm to take into account the energy of the selected paths while maintaining the security and trust of the route. We shall refer to the energy aware trust–based multipath algorithm with message security scheme as E-TBM.

1.3 Approach

The approach involves combining the following techniques to achieve our goal:

1. A trust assignment mechanism is used to assign a trust level to each of node based on whether it is involved in the data routing process.

2. A soft encryption technique is used to break the message into parts to be routed further into separate multiple paths.

3. A power-aware metric is introduced in the route selection process so that each node involved in the selected routing paths has an energy cost that determines the amount of energy consumed by that node when it transmits the data packet.

The above design features allow for determining the energy consumption necessary to maintain an acceptable level of message security in the network, and thereby to prolong the network lifetime.

1.4 Thesis Contributions

The contributions of this thesis are twofold:

1. We have developed an energy-aware secured routing protocol for MANETs (so-called E-TBM) through enhancing an existing message security scheme for MANETs (so-called TBM [1]) by introducing an energy constraint within its routing process so as to produce a network with improved lifetime.

2. We have carried out a performance evaluation to validate our proposed scheme (so-called E-TBM), demonstrating its effectiveness in saving energy consumption and increasing the network lifetime.

1.5 Thesis Organization

The remainder of this thesis is organized as follows:

- **Chapter 2** describes some background work on MANETs and the DSR routing protocol. Approaches to achieve energy efficiency, and techniques that incorporate secured routing for MANETs are also discussed.

- **Chapter 3** presents a detailed description of the methodologies of our proposed E-TBM scheme.

- **Chapter 4** presents our simulation results of the proposed E-TBM scheme.

- **Chapter 5** concludes our work and highlights some future research on the studied topics.

Chapter 2

Background And Related Work

2.1 Background

2.1.1 Mobile Ad Hoc Networks

MANETs are a type of network where nodes collaborate with each other to guarantee proper communication between them. This is achieved without the presence of centralized entities that can monitor the operations of these nodes. Due to its dynamic topology, the links in a MANET can be established and broken continuously depending on the velocity, direction, and transmission range of nodes. Contrary to wired networks, nodes in a MANET have no fixed infrastructure and thereby, they are limited in communication range. Typically, intermediate nodes are forced to forward the packets in those cases where the destination node is not within the transmission range of the source node.

We depict a wireless network in Figure. 2.1 where the nodes communicate through a router. Typically in this setting, the wireless devices can communicate only if the wireless router gives them permission and control to do so. In contrast, we depict a MANET with wireless nodes communicating with each other in Figure. 2.2. In such a network, nodes communicate with each other, and are not governed by a single node or entity.

Our scenario is based on such network, which has the following assumed features:

1. A node has the capability to function as both a host and a router.

2. Control and management of the network is distributed among the nodes.

3. In case no direct route is available to deliver the data packets from a source node to its destination node, these packets should be forwarded via one or more intermediate nodes.

4. Due to mobility of nodes, the connection between mobile nodes may vary with time.

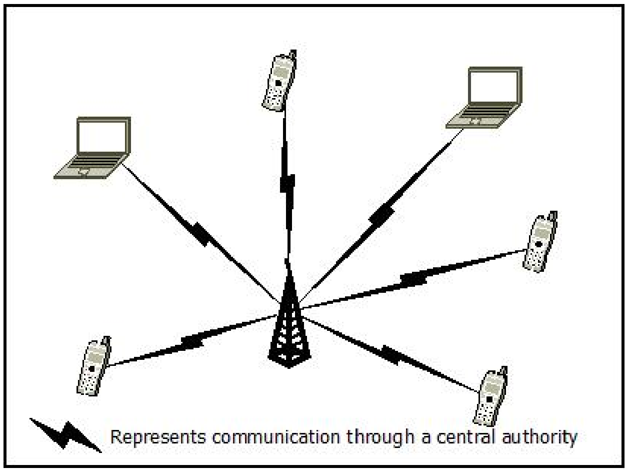


Figure 2.1: An example of a wireless network

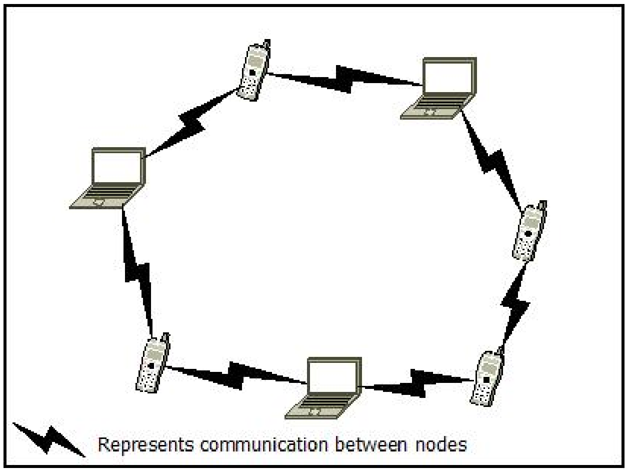


Figure 2.2: An example of a MANET

2.1.2 DSR Protocol

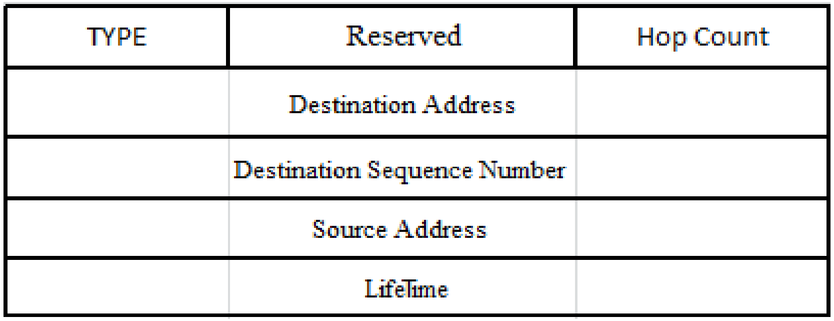
In traditional wireless networks, including MANETs, routing protocols can typically be categorized in different ways: including global/proactive, on demand, reactive and hybrid [3, 4]. For proactive routing protocols, routes to all of the destination nodes in the network are determined in the beginning when nodes are turned on and maintained by a periodic update process of the available routing paths. For reactive protocols, the routes in the network are determined when a source node wants to route its data packets to a specific destination node using a discovery process. Hybrid routing protocols employ the concepts of both proactive and reactive protocols [3] to achieve data routing.

Table driven protocols do not scale well in large MANETs because frequent route updates would consume expensive bandwidth, increase the channel contention, and cause the power of each node to deplete by a considerable amount. Since in our investigation, power consumption is very important; we use a modified reactive routing protocol (so-called Destination Source Routing Protocol (DSR)).

The standard DSR Protocol is a simple destination source routing protocol that consists of two processes [5]: *Route discovery* and *Route maintenance*.

When a source node sends a message packet to an intended destination node, it first sends a Route Request (RREQ) packet to all nodes in the network through a broadcast. When all intermediate nodes on the network receives this RREQ, they append their own unique identifier to the RREQ packet. If the destination node is found within an intermediate node's routing table, the source node will forward the packet to that node. If no entry is found in that routing table, the node will simply forward the request to the rest of its neighbors but will still append its unique identifier in the RREQ packet header. With this being done, the destination node knows all the intermediate nodes it will need to traverse along the route to send the acknowledgment of receipt (ACK), back to the source node. The RREP packet header of the original DSR routing protocol is depicted in Figure. 2.3.

At this stage, when the destination node is found, it will use the packet header as mentioned previously to reply with a Route Reply (RREP) to the source node, and this lets the source node be aware of the full availability of the discovered route to be taken.



TYPE	Reserved	Hop Count
	Destination Address	
	Destination Sequence Number	
	Source Address	
	LifeTime	

Figure 2.3: Original RREP packet format

The reason the *Route Maintenance* exists is because in MANETs, the network topology is constantly changing, meaning that nodes can enter or leave the network at any given time. Due to this nature, the source node is informed of this change by means of a Route Error packet (RERR). When this happens, it means that a break in the route has occurred, and the source node will then use an alternate route to send its information to the destination node (this refers to the multipath property of DSR used in this thesis). The routing information is stored in the route cache and if such information exists, the source node initiates the Route Discovery process again [5, 6]. In our implementation of the multipath DSR routing, we modify the route discovery process introduced in [1] to incorporate node energy constraint (see Chapter 3).

2.2 Energy-Efficiency as a Key Concern when Designing Multipath Routing for Wireless Ad hoc Networks

When considering a number of advances that have occurred in wireless communication technologies worldwide such as Bluetooth, WiFi, WiMax, FM radio and Near Field Communication (NFC), mobile ad hoc networks have generated a lot of interest in the recent years [7] since these networks are infrastructure-less and can greatly benefit from connecting the nodes (i.e. power-aware devices) in such networks using multipath routing features provided through the use of the technologies, from an energy efficiency perspective.

There are many consequences of routing messages in such a network from node to node over a wireless transmission medium, such as noise, interference and also importantly, when the power of a node is low or costly; the energy efficiency becomes a concern [8] since this factor relates to the design and operation of such a network. If nodes can no longer communicate in such an environment because they've run out of power, loss of communication can be detrimental to the parties that are involved.

Routing in MANETs is a challenging task due to node mobility, limitations in bandwidth transmission, battery power, and CPU time. In a MANET, each node communicates only with those nodes that are within its communication range, and the destination node may be reached after multiple hops. Therefore, the death of a few or a single node due to energy exhaustion can cause communication breakdown, thereby disrupting the entire network routing operation. It should also be noted that when performing routing in multipath MANETs, for any active connection, the source node, as well as the well as the intermediate nodes and the destination node may change their position due to their mobility, which means that the paths selected for routing the messages are potentially subject to frequent disconnections. In such situations, it would be necessary to decrease the disruptions caused by the changing topology. The above-mentioned constraints are considered in our work when designing our energy-aware and secured routing scheme for MANETs.

2.3 Approaches To Achieve Secure Energy-Efficient Routing in Wireless Ad Hoc Networks

Efficient routing in MANETs is required to properly deliver the packets to their intended destinations with minimal delay while extending the lifetime of the network through energy efficient selection of the routes.

In our investigation, we have found a clear distinction in the types of research currently being undertaken. Research with Energy-aware routing protocols for MANETs and Energy-aware secured routing protocols.

2.3.1 Energy-Aware Routing Schemes for MANETs

Many routing schemes have been investigated in the literature that deal with energy efficiency. Most of these schemes directly involve modifying the standard AODV or DSR routing protocols, with the aim to increase the energy efficiency in the networks without taking into account the secureness of the data packets transmission [9–16]. Representative such schemes are discussed as follows.

In [9], Adoni and Joshi modified the Optimized Link State Routing (OLSR) routing protocol with the shortest hop routing method for data transmission, but instead of using one route, they use multiple paths so as to avoid congestion. They call their algorithm Modified OLSR with multipath (OLSRM). Using alternate paths in turn decreases the energy expenditure of nodes or makes them uniform. Performance metrics were used to evaluate their implementation such as number of nodes alive versus nodes' velocity, average end-to-end delay and nodes' speed versus routing overhead. They compare their results to that of OLSR and they obtained a 10-25% increase in node velocity and 5-10% increase in routing overhead.

In [10], Suganya et al. introduced a technique to maximize the lifetime of nodes by introducing a threshold value for each node that determines whether nodes are considered in the routing decisions with packet lengths considered to allow for equal power being consumed. In terms of simulations, they looked at the power consumption, packet drop ratio, and the end-to-end delay. Their investigation was successful as it showed an overall gain in terms of energy consumption the network.

In [11], Al-Gabri et al. defined a new routing protocol called Local Energy Aware AODV protocol(called LEA-AODV), which reduces the energy consumption by taking into account the initial energy of a node, the transmission power of the node, and the reception power of the node. These metrics are calculated and used to evaluate whether a power hungry node will conserve power by not forwarding data packets on behalf of others. Their simulations were based on (1) max speed and total energy consumption, (2) pause time and total energy consumption, (3) maximum speed and network life time, and (4) pause time and network life time. Their results showed that the life time of the network can be prolonged substantially.

In [12], Hiremath and Joshi proposed a protocol based on Adaptive Fuzzy Threshold

Energy (AFTE) that balances the energy usage of all nodes by load distribution and that the select routes with underutilized nodes rather than the shortest routes. Therefore packets are only routed through paths that have energy-rich intermediate nodes.

In [13], Rout et al. proposed a way of adjusting the topology of the network by controlling the transmission power of nodes in such a way that the node with the farthest transmission range takes part in the routing. Also the power of neighbouring nodes are varied during communication. Their simulations considered the total energy consumption versus the number of packets, the throughput and the average end-to-end delay. They found that their algorithm is good at energy conservation and performs better in average end-to-end delay without affecting the overall throughput of the network.

In [14], Kumar et al. introduced a new algorithm called Energy Aware Efficient DSR (EAEDSR) that avoids link breaks since they are energy consuming and uses routes according to the link and node stability. The node's stability used two metrics for calculation: the link expiration time and the remaining energy of the node. When combined, these metrics are used to reduce the cost of handling link breaks.

In [15], Verma et al. proposed a way to maximize the lifetime of MANETs by avoiding nodes with low energy and nodes that have more buffered packets than others in the network. They also optimized the energy consumption by varying the transmission range of the nodes. The performance metrics chosen were total energy consumed versus number of connections with varied pause times. They showed a 10-20% reduction in energy consumption and a 10% increase in the lifetime of the network. This improvement is done without increasing the routing overheads.

In [16], Anand and Prakash introduce an Energy Efficient DSDV (EEDSDV) Routing protocol that controls the transmission energy by varying the transmission power of nodes. In their proposed scheme, all RREP packets are not forwarded through all available nodes as done in the standard DSDV. The effectiveness of their proposed scheme in terms of energy consumption, end-to-end delay, and packet delivery ratio is proven.

In the next section, we describe representative energy aware secured routing schemes for MANETs.

2.3.2 Energy-Aware Secured Routing Schemes for MANETs

Secured routing protocols for MANETs [17] have been the subject of interest to the research community in the recent years. These protocols have been designed to satisfy the primary principles of network security, i.e. confidentiality, integrity, and availability, each having its own dynamics for achieving such goal.

In general, secured schemes for MANETs [17] can be classified as

1. Credit-based schemes [18–20] - where credits are used as incentive to encourage the nodes in participating towards the packets forwarding.

2. Reputation-based schemes [21] - where reputation values are assigned to nodes on the basis of a monitoring mechanism. These reputations are then used to assess their behavior with respect to their involvement in the data routing process.

3. Tit-For-Tat (TFT)-based systems [17] - where each node uses a TFT strategy to decrease or increase its service to its immediate neighbors with respect to data forwarding.

4. Cryptography-based systems [22–25]- where cryptography techniques are used to design security mechanisms for MANETs.

5. Trust-based multi-path schemes [1, 26, 27] - where trusted multipaths are used to securely route messages in MANETs.

In this thesis, the focus is on message security schemes based on trust-based multi-paths routing, where energy constraint is directly embedded in the design approach. Apart from relying on the proper selection of hardware, such approaches must also involve the study of coupling among layers of the system [28] since energy consumption does not occur only through transmission, but also through processing [8].

Following this trend, energy-aware secured routing schemes can be classified into schemes that promote:

1. The design of routing paths with minimal energy cost [29,30].
2. The design of routing paths that avoid (as much as possible) nodes with minimum remaining battery capacity [31,32].
3. The design of minimal energy cost paths made of nodes with a battery level higher than a prescribed threshold [33,34].
4. Schemes where routing paths are selected according to the remaining battery capacity at each node, the sending rate per node, or the energy cost of hops [35].

Representative such schemes are as follows along with other security based implementations that take energy into account.

In [36], Sheng et al. introduced a DSR-based energy efficient routing protocol for MANETs (called NCE-DSR) which uses the number of times that a node sends the messages as a parameter for deciding on the inclusion of this node in the selected routing path. A routing cost function is designed for determining the choice of the routing path. However, the overhead generated from this method is not revealed.

In [37], Vadivel and Bhaskaran proposed an energy-efficient and secured routing protocol (called Intercept Detection and Correction (IDC)) for MANETs. The IDC algorithm identifies the malicious nodes by recognizing the selective forwarding misbehavior from the normal channel losses by means of a residual energy parameter. However, no clue is provided as to how this energy related parameter is determined.

In [38], Babu proposed an energy-based secure authenticated routing protocol (called EESARP) for MANETs. The EESARP scheme uses an attack resistant authentication combined with hop-by-hop signatures to mitigate the routing misbehavior of potential malicious nodes while improving the reliability of the route request packet. A node selection mechanism is also designed to ensure that the proposed routing protocol is power aware.

In [39], Taneja and Kush proposed an energy-efficient and authentic routing protocol (called EESSRP) for MANETs which incorporates security (by means of hash key generation and Diffie-Hellman protocol) and power features in its design.

In [40], Vadivel and Narasimhan also proposed an energy-aware and secured routing scheme for MANETs, where energy-efficiency is achieved by a technique for reducing the broadcast messages in the network.

In [41], Banerjee et al. proposed a trust based multipath OLSR routing protocol for MANETs (called ESRP) where trust is established by means of a signed acknowledgement based on asymmetric key cryptography. Digital signature in each acknowledgement packet is used to prevent the generation the of forged packets.

In [42], Saha et al. proposed an energy efficient scheme (called EEABSR) with secure routing by reducing the background network activity for the nodes to route data packets in the network. In their scheme, there are nodes that have different roles. These nodes are referred to as common nodes, associative nodes, administrator nodes, and watch nodes, that are used to monitor the network so as to determine whether a node will participate in data forwarding according to its trust and remaining battery power. Their evaluations are based on the number of packets dropped and the average power consumed. Their their algorithm is compared against AODV and DSR, showing better power consumption.

In [32], Kumari and Shrivastava proposed an algorithm for detecting the network intrusion for security and an energy efficient DSR based protocol which uses the minimum-hop fixed-power version of DSR. Their scheme uses nodes that have higher power to interact in the network, thus there is always a battery limit to observe while routing decisions are made. The performance metric used to validate their scheme is the transmission energy. Their results showed that according to the distance, the transmission power can increase or decrease; but the greater the distance, the more energy will be needed.

In [29], Kush and Taneja proposed an energy efficient schema based on power consumption states and secured routing by using a hash key chain mechanism that uses the AODV routing protocol to introduce a robust implementation. Their scheme is evaluated using a packet delivery fraction (called PDF) which defines the number of successful packet delivery. Compared to the standard AODV, their scheme is shown to be better in terms of packet delivery ratio.

In [43], Tamilarasi et al. proposed a double ACK mechanism as an add-on for the DSR routing protocol along with two cryptographic algorithms (digital signature algorithm and one-way hash chain) to secure the data transfer in MANETs. Their scheme is shown to outperform DSR in terms of end-to-end delay, packet delivery ratio, and routing overhead.

In [33], Gaikwad et al. proposed an energy-aware secure routing scheme that increases the lifetime of MANET while reducing the power expenditure during the route establishment. In their scheme, a cryptographic method is used, where only the secure nodes having the required energy level can participate in the route discovery and data transmission phases. Their simulation results showed positive results in terms of energy consumption efficiency even though the cryptographic method added some delay.

In [44], Vijayan et al. proposed a trust-based routing scheme for MANETs that takes into account the energy of nodes as they interact with each other. Fuzzy logic is used as a technique to evaluate the trust of a node and to detect misbehaving nodes in the network. The performance of their proposed scheme is evaluated using packet delivery ratio, throughput, and energy consumption as performance metrics, showing its effectiveness. However, this protocol was not compared against other existing benchmarks.

In [45], Gopinath, Rajaram and Kumar proposed a technique with a three phase approach to reduce the node energy consumption of highly mobile nodes, to limit malicious node activity, to reduce replaying of packets that could drain battery power, and to identify unidentified nodes using a digital signature verification scheme. Their proposed DSR-based protocol is shown to outperform DSR in terms of energy consumption, end-to-end delay, and routing overhead.

Unlike the above-described schemes, our proposed E-TBM scheme is a mimic of our recently proposed TBM scheme [1], where energy consumption at each node is now incorporated into the route selection phase, in order to decide on the secure route to be used to transfer the data packets.

Chapter 3

Methodology

As discussed in Chapter 1 and Chapter 2, MANETs by nature are made of mobile nodes which are often powered by a battery. Since energy conservation is important for practical applications purpose, the loss of messages becomes a serious problem. Due to this, we have implemented energy awareness into an existing secured multipath routing scheme [1]. In this chapter, techniques used for designing our energy efficient and secured routing scheme for MANETs (so-called E-TBM scheme) are described in-depth.

3.1 Enhanced Trust Based Multipath DSR Protocol With Soft Encryption Algorithm (E-TBM)

Lets assume that a source node, say S, wants to transmit a message, say m, to a destination node, say D, our E-TBM approach follows the same steps as the TBM approach [1] to securely send the message. A simple illustration of such interaction between two nodes is shown in Figure. 3.1. Basically, the message m will undergo a series of processes between the time it is issued by the source node S and the time it is received by the destination node D.

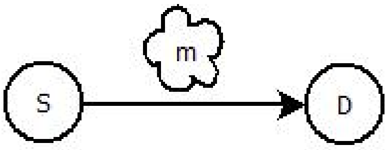


Figure 3.1: Basic Message sending between a source and destination node

Our E-TBM method consists of a combination of message encryption, energy-aware message routing using DSR, and message decryption, yielding an energy-aware secured multipath routing scheme for MANETs (as shown in Figure. 3.2).

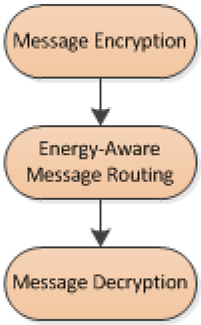


Figure 3.2: Proposed Message Security Scheme

3.1.1 Message Encryption

In a typical multi-path routing algorithm, a message is subdivided into n parts, of which k parts are required to decrypt the message, where $n \leq k$. The n parts are then routed using n different routing paths to the destination node. These paths are furnished by a conventional routing algorithm (such as DSR, AODV, etc).

In the proposed encryption scheme, the message m (at the source node) is segmented into four parts a, b, c, and d, then these paths are encrypted using soft-encryption - i.e. encryption based on the message itself. Typically, the following XOR operation on bits [1] is utilized, producing the message parts a', b', c', and d' as follows:

$$
\begin{aligned}
a' &= a\ XOR\ c \\
b' &= b\ XOR\ d \\
c' &= c\ XOR\ b \\
d' &= d\ XOR\ a\ XOR\ b
\end{aligned}
\tag{3.1}
$$

Using soft-encryption helps avoiding the problem of key exchange between the sender (source node) and the receiver (destination node) since in this case, the message parts are themselves used as the keys.

3.1.2 Energy Aware Message Routing Using DSR

In this step, the encrypted message parts a', b', c', and d' are routed using a modified multipath DSR protocol. Our message routing scheme uses a combination of a Trust Assignment Strategy, and a modified DSR Routing Mechanism that incorporates power costs to determine the best routes.

3.1.2.1 Trust Assignment Strategy

Our trust mechanism is inspired from the works described in [27, 46], which promote the idea of identifying malicious nodes through node actions and packets monitoring, then using this detection method to either increase or decrease the node's trust value. A node observes each of its neighbors to which its packets can be transferred and assigns a trust value to each of these neighbors in a dynamic way [1, 46, 47] based on the acknowledgments, as well as the trust recommendations (piggybacked on DSR routing packets) received from its peers regarding each neighbor node.

To help understand how trust values are assigned to nodes, let's consider the typical example shown in Figure. 3.3.

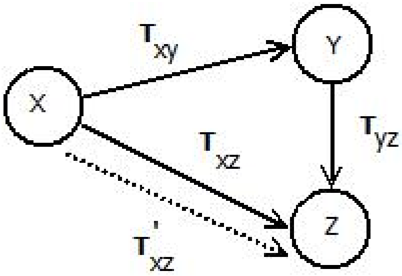


Figure 3.3: Assignment of Trust Values to Nodes

The trust assigned by node x to node z (denoted Trust_xz) is obtained [1] as:

$$\begin{aligned} &Trust\_xz = 1 – (1 - Trust\_xz)(1 - Trust\_xyz) \\ &where\ \ Trust\_xyz = (1–(1 - Trust\_xy)^{Trust\_yz}) \end{aligned} \tag{3.2}$$

It should be noted that due to node mobility, whenever a new node joins the network, it will send a HELLO packet to all its neighbors, and these neighbors will then assign an initial trust value of 0 to that new node. The trustworthiness of this new node will further increase (case where the node shows a benevolent behavior) or decrease (case where the node shows a malevolent behavior). On the other hand, when an existing node leaves the network, it will no longer respond to messages, and can be deleted from the routing tables of all nodes.

Once trust values are assigned to all nodes, these values are then normalized into integer discrete values in the range [-1, 4] using Equations (3.3) and (3.4). A trust level of 4 defines a complete trust and a trust level of -1 defines a complete distrust, meaning that that any packet coming from a node with trust level of -1 should be dropped. No packet should in turn be routed to this type of node (malicious node), leading to its isolation. These trust levels also define the maximum number of packets that can be routed via nodes.

The following formula is used for converting trust values from the range (y_{max}, y_{min}) to the range (x_{max}, x_{min}):

$$x = x_{min} + ((y – y_{min})((x_{max} – x_{min})/(y_{max} – y_{min}))) \tag{3.3}$$

Assuming that the maximum trust value (denoted t_{max}) and the minimum trust value (denoted t_{min}) in the network are known, let $x_{max} = 4$ and $x_{min} = -1$. If t denotes the actual trust value of a node and t_{norm} denotes the normalized trust value, Equation 3.3 will yield

$$T_{norm} = -1 + ((t – t_{min}) * (5/(t_{max} – t_{min}))) \tag{3.4}$$

In our simulations, we have used the values $t_{min} = -80$, and $t_{max} = 28$; obtained through observations.

Using these normalized trust values, a trust-based path selection strategy is utilized, governed by the policy that a node in the selected routing path cannot be granted more encrypted message parts than its assigned trust level would allow. In order words, a path p with trust T_p can be given only T_p parts of the packet to forward. This rule helps recognizing more trusted nodes, to which more encrypted message parts of the message should be granted. This way, non-trusted routes that may use brute force attacks to decrypt messages travelling through the network are likely to be avoided.

3.1.2.2 Energy-Aware Routing Mechanism

When a source node needs to route a message to a destination node, a route request (RREQ) packet is broadcasted. If a neighbor node that replies to the RREQ has the route to the destination or if the packet reaches the destination node, a route reply (RREP) is sent back to the source node acknowledging a successful delivery. In the packet header, the RREP message and trust levels of the previous nodes involved in the packet forwarding are recognized and sent backwards along the routing path selected by DSR. The current battery level (energy) of a node (computed as shown in Equation (3.5) [2]) is added to the packet header.

$$E_j(t) \; = E_j(0) \; - \; \left(\sum_{t=0}^{G_j(t)} (CR(\tau) + CT(\tau)) \right) - \left(\sum_{t=0}^{X_j(t)} (CR(\tau) + C_p(\tau)) \right) - \left(\sum_{t=0}^{R_j(t)} (CR(\tau) + C_p(\tau) + CT(\tau)) \right) \tag{3.5}$$

where

- E_j(t) represents the current battery level (energy) of a node j at time t.
- $E_j(0)$ represents the initial battery level (energy) of a node j.
- G_j(t) is the number of packets generated by node j up to time t.
- X_j(t) is the number of packets received by node j up to time t.
- R_j(t) is the number of packets relayed by node j up to time t.
- $C_p(\tau)$ is the processing power cost of packet τ.
- CT(τ) is the transmitting power cost of packet τ.
- CR(τ is the receiving power cost of packet τ.

The E-TBM algorithm uses the following process to find the secure routes from a set of given routes:

1. The multiple paths are calculated by DSR, by waiting for a specified period of time for the multiple RREP packets to come from various paths. When a new route is found, they are arranged in increasing order of hop-counts and descending order of trust levels. This step is to ensure that the selected routes are of least hop-count besides being most trusted, so as to minimize the routing overheads. Two counters are set, one to keep

track of the selected nodes in the selected routing paths, and the other to keep track of the nodes' power levels.

2. The first route is selected and it is assumed that the maximum number of message parts that can be routed through it have been routed. Note that no actual routing is done at this step.

3. The next route is selected and it is assumed that the maximum number of message parts that can be routed via it have been routed. If all the parts of message can be routed securely, the actual routing is done by using the selected paths.

4. If four paths have been selected out of all possible combinations of paths, arrange these paths in terms of their energy that each would require to send the data packets.

5. Select the path that has the smaller energy path value. Out of the remaining paths, use the next lowest path energy, and so on.

6. Repeat this process until thr secured routes are found.

7. If no secured routes are found, the algorithm is repeated by starting at Step 2, by selecting a second route (alternate route) as the first route.

8. This algorithm is repeated until all the combinations of the paths are exhausted. If no secured route is found, the algorithm waits for another route. If all routes have been found or a specific time interval has expired, it is assumed that the algorithm has failed. An error message is then generated.

The pseudo code of the E-TBM algorithm is shown in Algorithm 1.

Algorithm 1 E-TBM

```
Arrange the paths P=$P_1$, $P_2$, ...,$P_n$ in increasing order of hop counts and descending order of trust levels
Initialize Count $C_j$ for all nodes to 0
Initialize Count $E_j$ for all nodes energy value to 0
Select the smallest path from P
if ∀ selected nodes j, $C_j \leq T_j$ then /*$T_j$ is the trust level of node j*/
    if four paths are selected then
        if ∀ selected nodes j, $E_j \leq Threshold\_E_j$ then /* Threshold_$E_j$ is the threshold on node energy values and $E_j$ is determined by Equation 3.5.*/
            Select path with smaller energy value
        end if
        Select the next smallest path with lowest energy
    else
        Continue
    end if
    if All paths are exhausted then
        Wait for another path
    end if
    if No Paths are left then
        Print ”Not possible to route securely”
    end if
end if
```

The E-TBM route selection algorithm (Algorithm 1) has a worse case complexity of $O(n^m)$ where n is the number of paths and m is the number of message parts.

Now, let's illustrate our modified DSR schema using an example.

We consider a scenario with 8 nodes as depicted in Figure. 3.4. Nodes A through H follow the standard routing process of DSR with the source node A initiating a broadcast RREQ to the destination node H. When any of these intermediate nodes C, B, D, E, F, G encounters this RREQ and has the destination node information in its route cache, it will append its trust value and energy required to get to that point in the RREP packet header. If the destination node H is found, it initiates a RREP to the source node. The selection of the secured routes with the least energy will be determined that way and the message will be routed along those secured paths. This scenario is shown in Figure. 3.4 and for simplicity, we have omitted all of the RREPs seen other than the path traversed in A, C, D, F and H. The modified RREP packet structure is illustrated in Figure. 3.5.

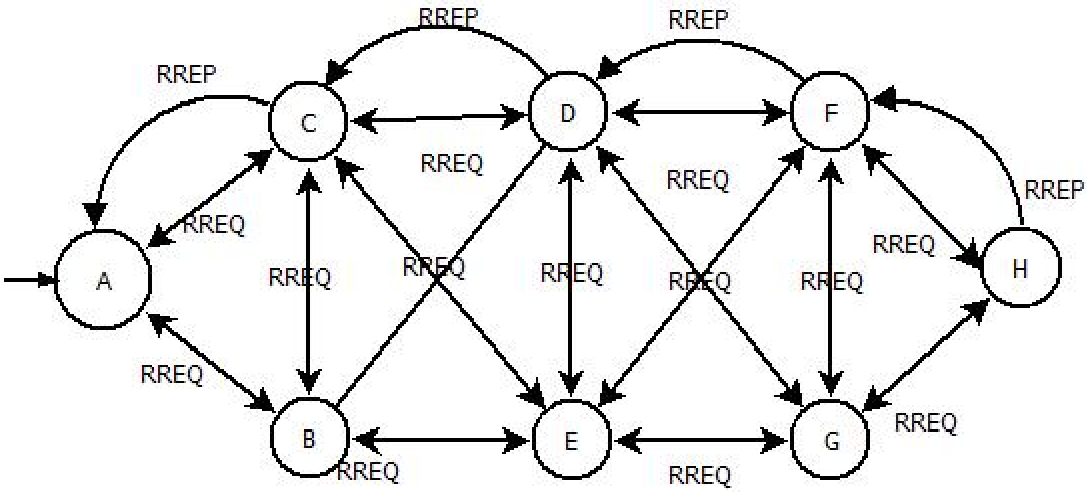


Figure 3.4: Illustrating the DSR protocol

TYPE	Reserved	Hop Count
	Destination Address	
	Destination Sequence Number	
	Source Address	
	LifeTime	
	Trust Value	
	Battery Power	

Figure 3.5: RREP packet format

A flowchart describing the E-TBM routing scheme operations is given in Figure. 3.6

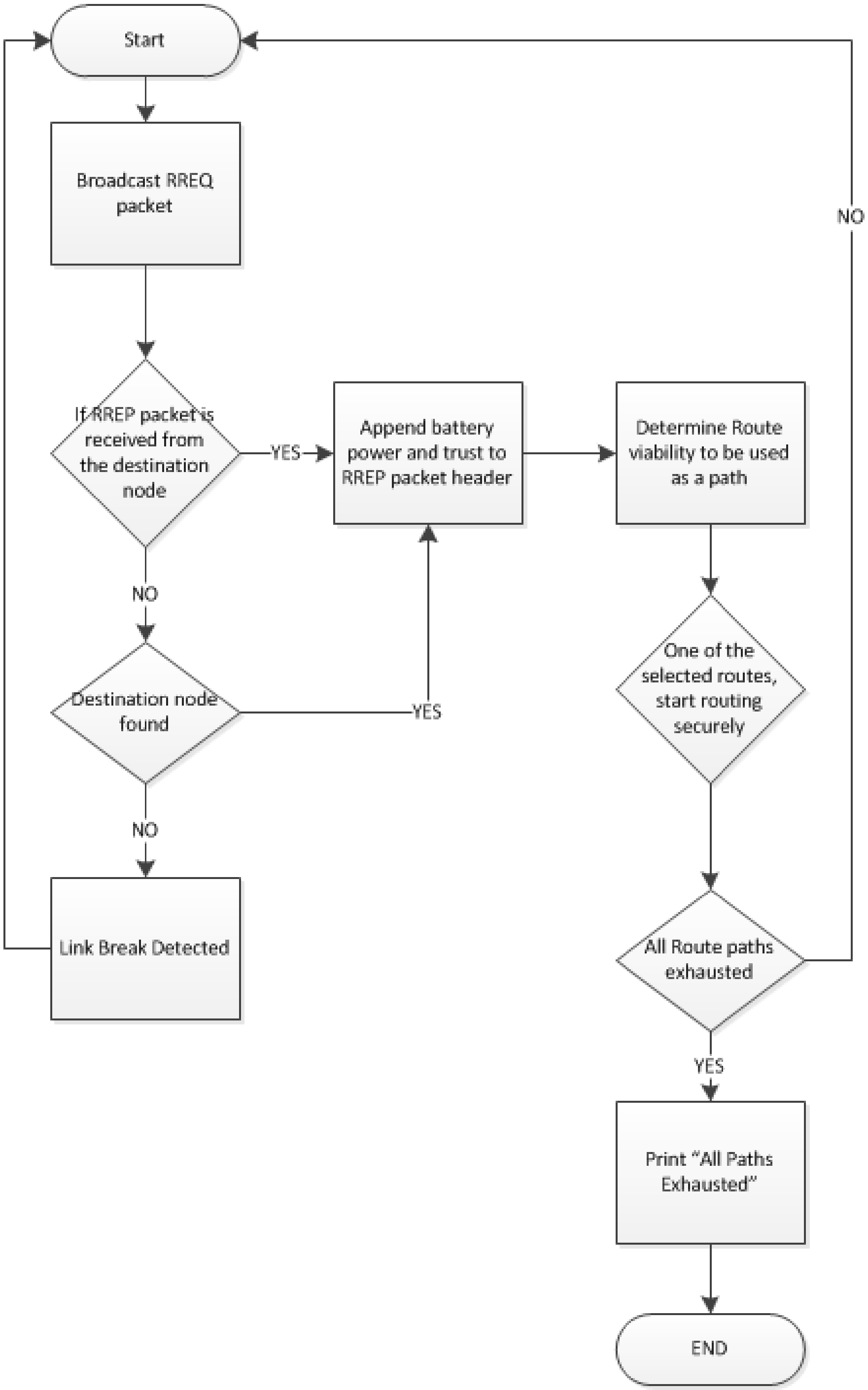

Start
Broadcast RREQ packet
If RREP packet is received from the destination node
YES
Append battery power and trust to RREP packet header
Determine Route viability to be used as a path
NO
Destination node found
YES
NO
Link Break Detected
One of the selected routes, start routing securely
All Route paths exhausted
NO
YES
Print "All Paths Exhausted"
END

Figure 3.6: E-TBM routing scheme operations

3.1.3 Message Decryption

At the destination node D, the encrypted message parts a', b', c', and d' are decrypted to recover the original message m as follows [1]:

$$\begin{aligned}
&a = b' \, XOR \, d' \\
&b = a' \, XOR \, b' \, XOR \, c' \, XOR \, d' \\
&c \;=\; a' \, XOR \, b' \, XOR \, d' \\
&d \;=\; a' \, XOR \, c' \, XOR \, d'
\end{aligned} \tag{3.6}$$

Chapter 4

Performance Evaluation

In this chapter, the performance evaluation of out proposed E-TBM scheme is compared against that of the TBM scheme [1] using several performance metrics. Our results are validated through simulations.

4.1 Simulation Tool

We use the Global Mobile Information System Simulator (GloMoSim) simulation tool [48], where soft encryption using multiple message parts is implemented at the application layer. The GloMoSim program is an environment that is scalable for large wireless and also wired communication systems. It uses the parallel discrete-event simulation language called PARSEC [49].

GloMoSim is an event based system which is coded in the C language. It implements all the 7 layers of the OSR reference model [50]. In addition, it supports pre-compiled models and protocols at the various levels including the DSR routing protocol at the network layer, upon which our study is based. At the Medium Access Control (MAC) layer, there are available protocols such as CSMA, FAMA, MACA, and IEEE 802.11. At the application layer, there are traffic models that are available such as TCPLIB, CBR (Constant Bit Rate) and FTP and HTTP. In our implementation, we use CBR at the application layer and we implement the soft encryption using multiple message parts at the application layer as well.

We also assume that the trust levels of nodes are available to the source nodes. The remaining simulation setup is given in Table. 4.1 (in Section 4.4).

4.2 Performance Metrics

The following performance metrics are used for the evaluation of our proposed scheme:

- *Route selection time*: this represents the total time required for the selection of a routing path, i.e. the time taken from the beginning of the route selection process, till the route is computed.

- *The trust compromise*: this represents the sum of access violations in all the paths selected for routing.

  The access violation at node n is defined as the difference between n_{parts}, the number of encrypted message parts that n has received and T_n, the trust level of n if $n_{parts} \geq T_n$, i.e. if N_p is the set of nodes in a routing path p, the trust compromise for path p is obtained as:

  $$TrustCompromise_p = \sum_{n \in N_p} (n_{parts} - T_n) \tag{4.1}$$

  wherever $n_{parts} \geq T_n$ and T_n is the trust assigned to node n and n_{parts} is the number of encrypted message parts received by node n from all the paths. The aggregate trust compromise is calculated for all the paths selected for routing. It therefore means that a node can never have more parts than its trust level.

  According to the lemma presented in [1], the trust compromise of the selected routes for soft encryption and trust based, multi-path routing is always zero.

It has been demonstrated from the Equation 4.1 and the lemma presented in [1] that the trust compromise of the selected paths in the E-TBM scheme is always equal to zero because a node cannot have more parts n_{parts} than its trust level T_n.

- *The number of dead nodes*: a dead node is defined as a node which has completely depleted its power level. When a node is drained of all its available power, it no longer plays a role in the route selection process.
- *Total energy consumed by the selected routing paths*: this represents the sum of energy consumed by the nodes that are chosen to be part of the selected routing paths.
- *Total energy consumed in the network*: this represents the sum of energy consumed by all the nodes in the network, regardless of their involvement in the route selection process.

4.3 Assumptions

In our simulations, we assume all nodes in the network are working normally and start off with a predetermined energy value of 5000 Joules. The nodes are uniformly placed over the specified terrain dimensions and are stationary. When a node runs out of battery power, it will no longer take part in the route selection process.

4.4 Simulation Parameters

Table. 4.1 outlines the simulation parameters used:

Table 4.1: Simulation Parameters

Parameter	Setting
Terrain Dimension	2000m x 2000m
Number of nodes	10 to 50 nodes
MAC Protocol	IEEE 802.11
Radio transmission power	Variable
Traffic Type	CBR
Simulation Time	600 s
Initial battery power of each node	5000 Joules

We have also included a sample GloMoSim configuration file in Appendix A which shows all the tune-able parameters and the ones that we have defined.

4.5 Simulation Scenario

In our scenario, 10-50 nodes were placed uniformly over the 2000m x 2000m terrain. When a source node initiates a RREQ packet to the destination node, it keeps track of the number of possible paths to that destination.

Upon reaching the destination node, the energy and trust are added to the packet header and sent back to the source node in the RREP packet. The source node then determines the routes that it will use to route the data (message parts) according the most trusted routes and the amount of energy.

The message is then encrypted and sent down the paths and decrypted at the destination node.

4.6 Simulation Results

First, we examine the total trust compromise for both the E-TBM and TBM schemes. The trust compromise of the E-TBM and TBM schemes are presented in Figure. 4.1. As expected, regardless of the number of nodes, the trust compromise of both schemes is equal to 0. This result is in agreement with the lemma presented and explained in [1]. The reason is that for both schemes, the routing paths are selected according to the policy that no node in such path can receive more encrypted message parts than its trust level would permit.

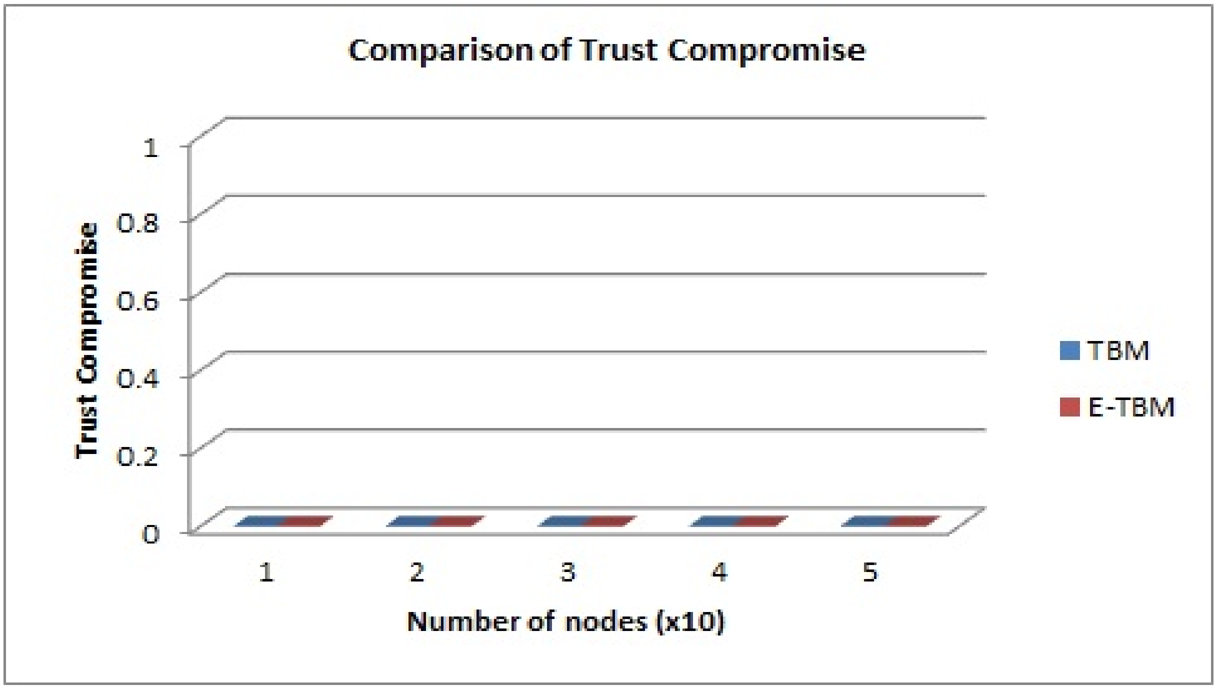


Figure 4.1: Comparison of Trust Compromise

Next, we compare the route selection times for both E-TBM and TBM schemes. The results are depicted in Figure. 4.2. In Figure.4.2, it can be observed that the route selection time for the E-TBM scheme has increased overall compared to that of the TBM scheme. This can be attributed to the fact that in the E-TBM scheme, more computation and time are required in selecting the paths with the least amount of energy while maintaining the route's security.

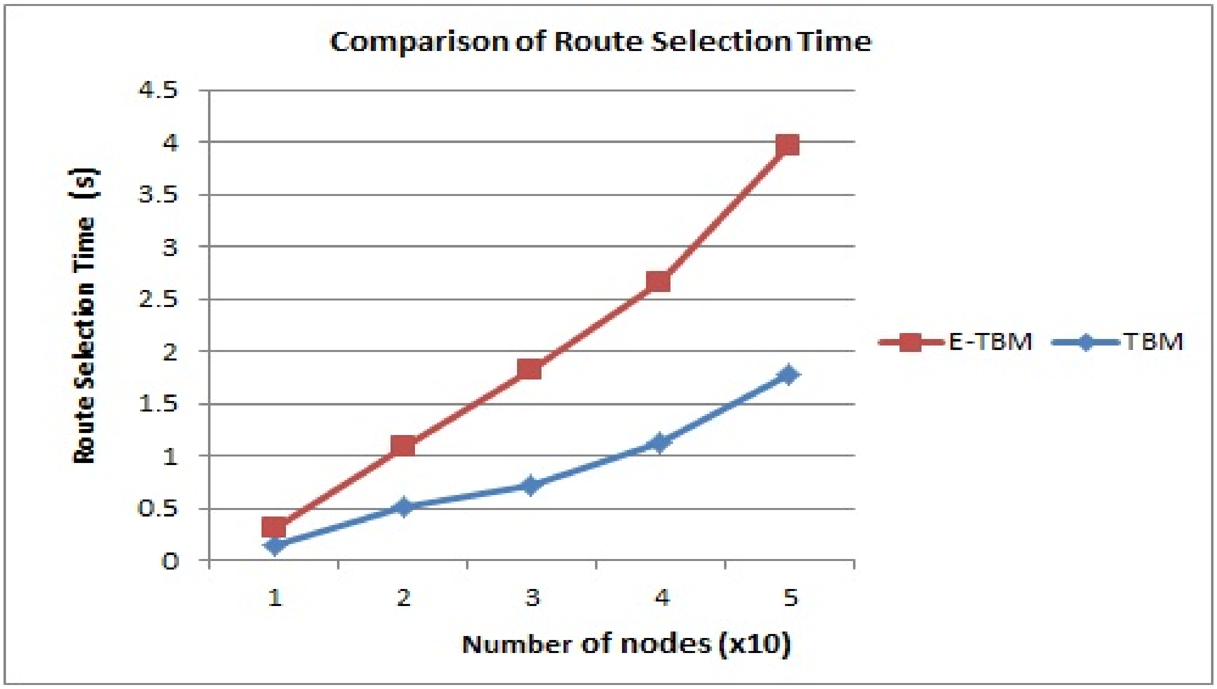


Figure 4.2: Route Selection time for E-TBM vs. TBM schemes

We also compare the total energy consumed (in Joules) by the nodes that are embedded in the selected secure paths for routing in both schemes. The results are captured in Figure. 4.3. In Figure. 4.3 it can be observed that the energy consumed in the case of the TBM algorithm is significantly higher compared to that of the E-TBM algorithm. This constitutes a justification of taking the energy required to transmit a packet into account when designing our secured routing protocol for MANETs.

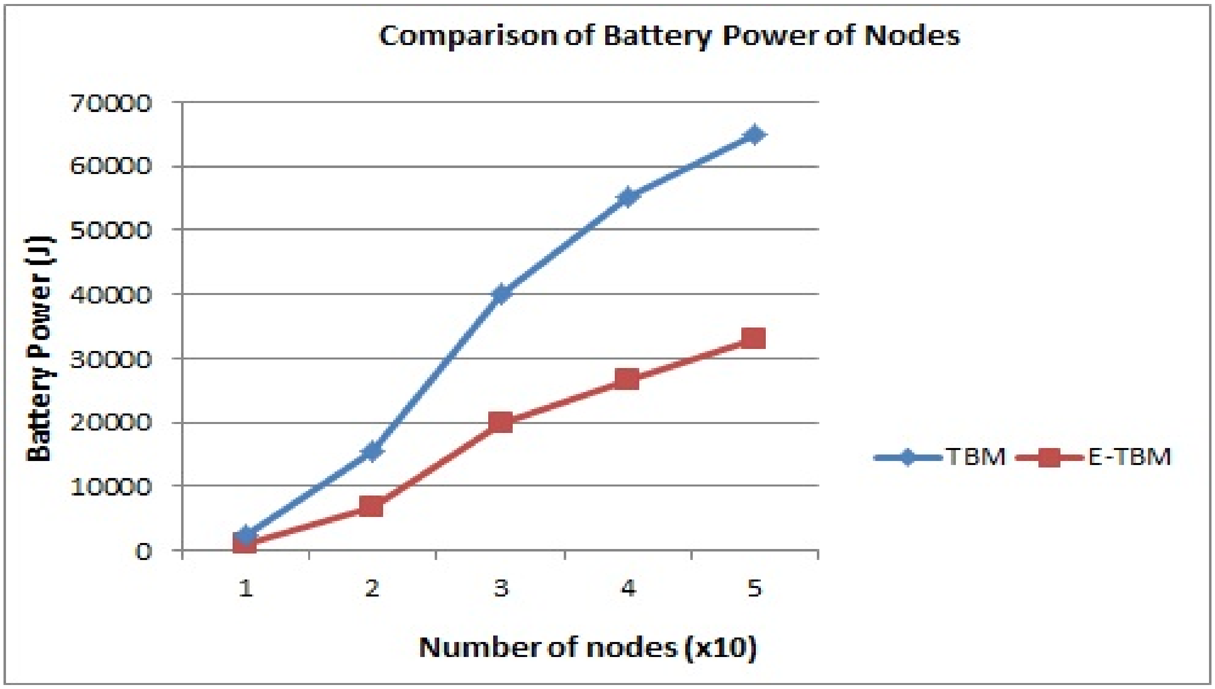


Figure 4.3: Total energy consumed in the selected routing paths for E-TBM vs. TBM schemes

Next, we compare the total energy (in Joules) consumed by all the nodes in the network, regardless of their involvement in the route selection process. The results are captured in Figure. 4.4. In Figure. 4.4, it can be observed that for the E-TBM scheme, the overall energy consumption required for multiple paths to be selected securely and for messages to be sent down those multiple paths is much lower than that experienced with the TBM scheme.

Our simulation is started with each node having 5000 Joules of power, which decreases according to the type of routing operation being performed and which involves that node. In Figure. 4.5, it can be observed that by the end of the simulation, there were fewer nodes that had depleted their power in the E-TBM scheme compared to the TBM scheme. This result is a direct correlation to the decreased total energy observed in the case of the E-TBM scheme. Since the total energy consumption is lower, nodes will survive longer, and therefore, the lifetime of the network will be increased.

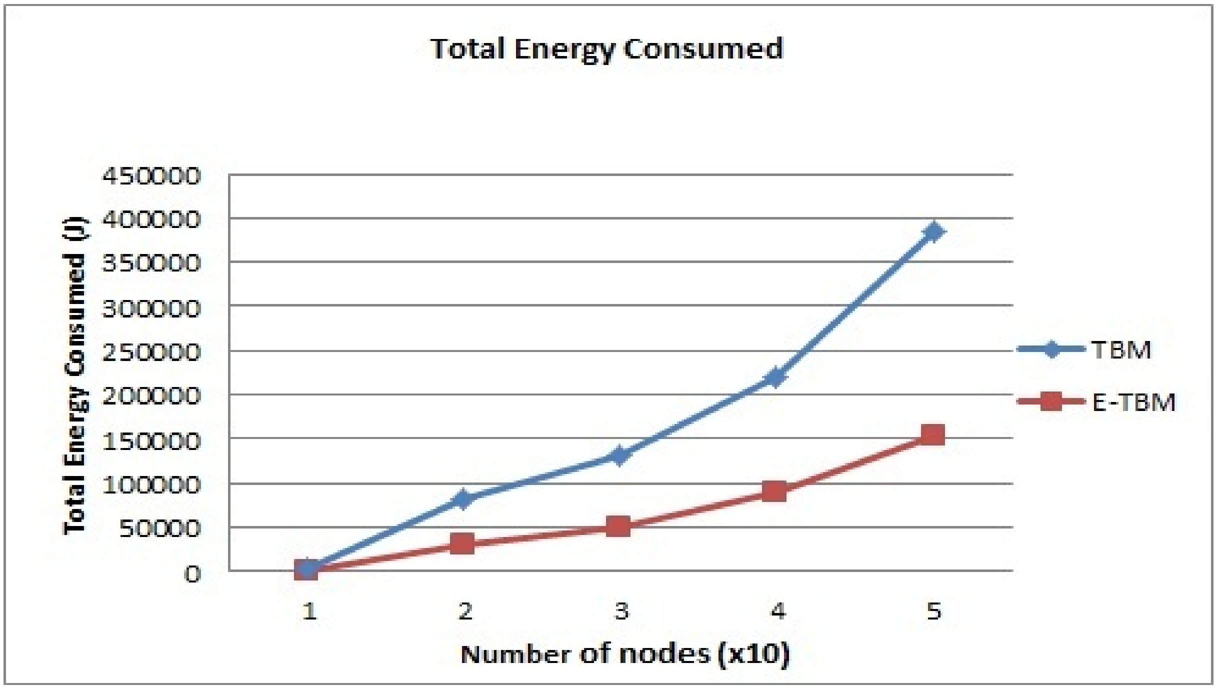


Figure 4.4: Total energy consumed based on E-TBM vs. TBM schemes.

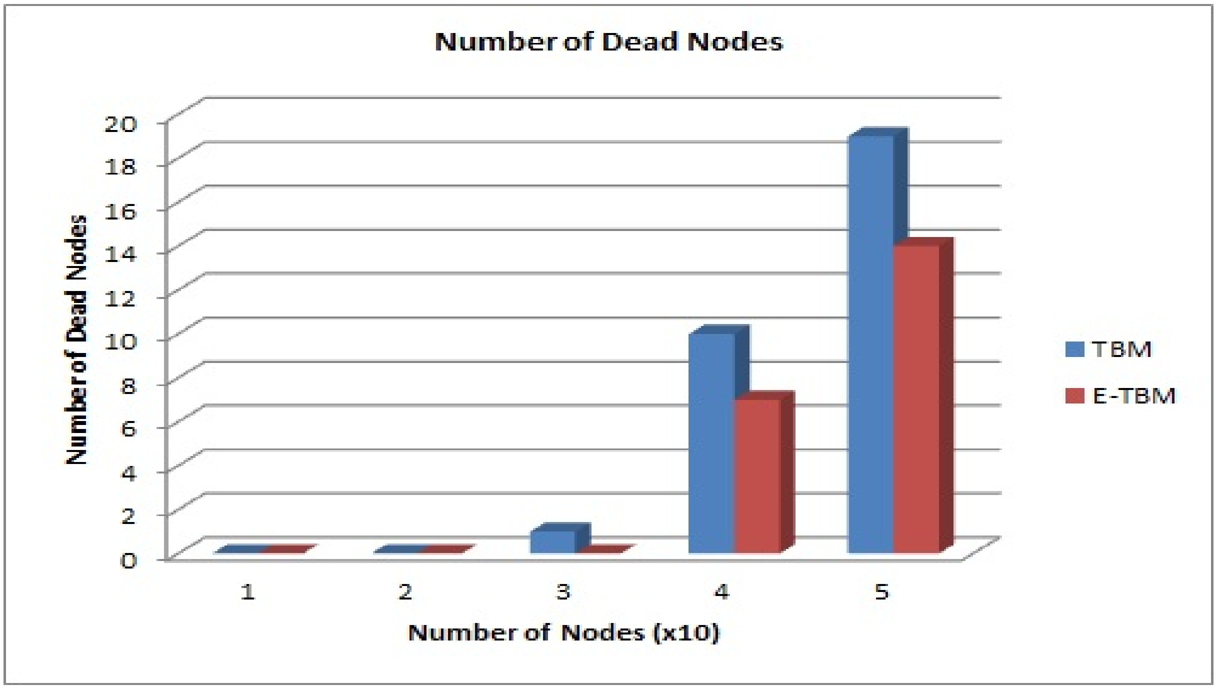


Figure 4.5: Number of dead nodes in the E-TBM vs. TBM schemes

Chapter 5

Conclusions

The main goal of this thesis was to help improve the energy efficiency of the route selection process in a secure trust-based multipath scheme. We first analyzed the different techniques available for achieving an energy efficient secured routing algorithm and were then able to come up with a technique to integrate a solution into a preexisting benchmark scheme (TBM scheme).

Our proposed DSR-based secured routing scheme for MANETs (so-called E-TBM) uses an energy-efficient secure path selection mechanism which minimizes the number of dead nodes, hence maximizes the network lifetime compared to the TBM scheme [1].

As part of future work, we intend to compare our scheme against other known energy-aware secured routing protocols in MANETs and other routing protocols such as AODV. We also intend to apply other encryption algorithms such as DES or AES as alternative encryption techniques and evaluate their performances.

Appendices

Appendix A

This appendix describes the GloMoSim software requirement specification for the implementation of our proposed E-TBM scheme and the TBM scheme. The Simulation intends to evaluate both schemes in terms of the performance metrics described in Chapter 4. In our simulations, the Medium Access Control (MAC) protocol (IEEE 802.11) is used, which defines the set of rules to coordinate the transmission of packets, re-transmission of damaged packets, and resolution among nodes.

A.1 Overview of the GloMoSim System

Our simulation considers n as number of nodes (between 10 and 50). The main objective is to update and store the neighbor table and routing table periodically and to use the energy value function given in Equation (3.6) to determine the node energy, and then the energy of every selected path for routing. When the routes are to be determined (using DSR) for communication between any two nodes, the route tables are searched for existing route between these nodes with the help of probing, the energy of each selected routing path is determined using Equation (3.6), and all the neighbor tables and route tables are thereby updated accordingly. The user can vary the various parameters such as number of nodes, terrain dimension and then study the performance of the above algorithms. Graphs depicted in the thesis show the results obtained.

A.2 Assumptions

- A node can listen to all the nodes within its transmission range.
- Nodes operate in half-duplex mode.
- Each node has an omni-directional antenna.

A.3 Interface Requirements

A.3.1 Command Line Interface

The following command can be invoked from the shell to run the simulator: *./glomosim config.in*

The configuration file would be in the format accepted by glomosim and would have all user configuration inputs apart from the standard input values in the sample configuration file of glomosim.

A.3.2 Software Resource Requirements

- Operating systems: Windows XP or higher/ Linux 32bit
- Language used: C
- Graphs generation: Microsoft Excel
- Network simulator: GloMoSim (built over PARSEC compiler)

List of input

1. **app.conf**

```
# The traffic generators currently available are FTP,
# FTP/GENERIC, TELNET, CBR, and HTTP.
#
```

```
#———————————————————————————————————————————————————————
# 1. FTP
#
# FTP uses tcplib to simulate the file transfer protocol.  In order to use
# FTP, the following format is needed:
#
#     FTP <src> <dest> <items to send> <start time> where
#     <src> is the client node.
#     <dest> is the server node.
#     <items to send> is how many application layer items to send.
#     <start time> is when to start FTP during the simulation.
#
# If <items to send> is set to 0, FTP will use tcplib to randomly determine
# the amount of application layer items to send.  The size of each item is
# will always be randomly determined by tcplib.  Note that the term ”item”
# in the application layer is equivalent to the term ”packet” at the network
# layer and ”frame” at the MAC layer.
#
# EXAMPLE:
#
#     a) FTP 0 1 10 0S
#
#         Node 0 sends node 1 ten items at the start of the simulation,
#         with the size of each item randomly determined by tcplib.
#
#     b) FTP 0 1 0 100S
#
#         Node 0 sends node 1 the number of items randomly picked by tcplib
#         after 100 seconds into the simulation.  The size of each item is
#         also randomly determined by tcplib.
#———————————————————————————————————————————————————————
# 2. FTP/GENERIC
#
```

```
# FTP/GENERIC does not use tcplib to simulate file transfer.  Instead,
# the client simply sends the data items to the server without the server
# sending any control information back to the client.  In order to use
# FTP/GENERIC, the following format is needed:
#
#      FTP/GENERIC <src> <dest> <items to send> <item size> <start time> <end time>
#
# where
#
#      <src> is the client node.
#      <dest> is the server node.
#      <items to send> is how many application layer items to send.
#      <item size> is size of each application layer item.
#      <start time> is when to start FTP/GENERIC during the simulation.
#      <end time> is when to terminate FTP/GENERIC during the simulation.
#
# If <items to send> is set to 0, FTP/GENERIC will run until the specified
# <end time> or until the end of the simuation, which ever comes first.
# If <end time> is set to 0, FTP/GENERIC will run until all <items to send>
# is transmitted or until the end of simulation, which ever comes first.
# If <items to send> and <end time> are both greater than 0, FTP/GENERIC will
# will run until either <items to send> is done, <end time> is reached, or
# the simulation ends, which ever comes first.
#
# EXAMPLE:
#      a) FTP/GENERIC 0 1 10 1460 0S 600S
#         Node 0 sends node 1 ten items of 1460B each at the start of the
#         simulation up to 600 seconds into the simulation.  If the ten
#         items are sent before 600 seconds elapsed, no other items are sent.
#
#      b) FTP/GENERIC 0 1 10 1460 0S 0S
#         Node 0 sends node 1 ten items of 1460B each at the start of the
#         simulation until the end of the simulation.  If the ten
#          items are sent the simulation ends, no other items are
#          sent.
#
#      c) FTP/GENERIC 0 1 0 1460 0S 0S
#          Node 0 continuously sends node 1 items of 1460B each at the
#          start of the simulation until the end of the simulation.
#------------------------------------------------------------------------
# 3. TELNET
#
# TELNET uses tcplib to simulate the telnet protocol.  In order to use
# TELNET, the following format is needed:
#      TELNET <src> dest> <session duration> <start time> where
#      <src> is the client node.
#      <dest> is the server node.
#      <session duration> is how long the telnet session will last.
#      <start time> is when to start TELNET during the simulation.
#     If <session duration> is set to 0, FTP will use tcplib to randomly determine
#     how long the telnet session will last.  The interval between telnet items
#     are determined by tcplib.
#
# EXAMPLE:
#      a) TELNET 0 1 100S 0S
#          Node 0 sends node 1 telnet traffic for a duration of 100 seconds at
#          the start of the simulation.
#
#      b) TELNET 0 1 0S 0S
#          Node 0 sends node 1 telnet traffic for a duration randomly
#          determined by tcplib at the start of the simulation.
#       ------------------------------------------------------------------------
# 4. CBR
# CBR simulates a constant bit rate generator.  In order to use CBR, the
# following format is needed:
#      CBR <src> <dest> <items to send> <item size>
#           <interval> <start time> <end time> where
#
#      <src> is the client node.
#      <dest> is the server node.
#      <items to send> is how many application layer items to send.
#      <item size> is size of each application layer item.
#      <interval> is the interdeparture time between the application layer items.
#      <start time> is when to start CBR during the simulation.
#      <end time> is when to terminate CBR during the simulation.
#     If <items to send> is set to 0, CBR will run until the specified
#     <end time> or until the end of the simuation, which ever comes first.
#     If <end time> is set to 0, CBR will run until all <items to send>
#     is transmitted or until the end of simulation, which ever comes first.
#     If <items to send> and <end time> are both greater than 0, CBR will
#     will run until either <items to send> is done, <end time> is reached, or
#     the simulation ends, which ever comes first.
#
# EXAMPLE:
#      a) CBR 0 1 10 1460 1S 0S 600S
#         Node 0 sends node 1 ten items of 1460B each at the start of the
#         simulation up to 600 seconds into the simulation.  The interdeparture
#         time for each item is 1 second.  If the ten items are sent before
#         600 seconds elapsed, no other items are sent.
#
#      b) CBR 0 1 0 1460 1S 0S 600S
#         Node 0 continuously sends node 1 items of 1460B each at the start of
#         the simulation up to 600 seconds into the simulation.
#         The interdeparture time for each item is 1 second.
#
#      c) CBR 0 1 0 1460 1S 0S 0S
#         Node 0 continuously sends node 1 items of 1460B each at the start of
#         the simulation up to the end of the simulation.
#         The interdeparture time for each item is 1 second.
```

```
#
CBR 0 14 100   256  5S   0S 150S
CBR 0 16 100   32  5S  90S 240S
CBR 0 19 100   1024  10S 120S 270S
CBR 0  6 100   64  10S 190S 340S
CBR 0 21 100   32  1S 210S 360S
CBR 0 13 100   512  2.5S 250S 400S
CBR 0 20 100   2048  5S 280S 430S
```

2. **config.in**

```
# ***** GloMoSim Configuration File *****

# Glomosim is COPYRIGHTED software.  It is freely available without fee for
# education, or research, or to non-profit agencies. No cost evaluation
# licenses are available for commercial users. By obtaining copies of this
# and other files that comprise GloMoSim, you, the Licensee, agree to abide
# by the following conditions and understandings with respect to the
# copyrighted software:
#
# 1.Permission to use, copy, and modify this software and its documentation
#   for education, research, and non-profit purposes is hereby granted to
#   Licensee, provided that the copyright notice, the original author's names
#   and unit identification, and this permission notice appear on all such
#   copies, and that no charge be made for such copies. Any entity desiring
#   permission to incorporate this software into commercial products or to use
#   it for commercial purposes should contact:
#
#   Professor Rajive Bagrodia
#   University of California, Los Angeles
#   Department of Computer Science
#   Box 951596
#   3532 Boelter Hall
#   Los Angeles, CA 90095-1596
#    rajive@cs.ucla.edu
#
# 2.NO REPRESENTATIONS ARE MADE ABOUT THE SUITABILITY OF THE SOFTWARE FOR ANY
#    PURPOSE. IT IS PROVIDED "AS IS" WITHOUT EXPRESS OR IMPLIED WARRANTY.
#
# 3.Neither the software developers, the Parallel Computing Lab, UCLA, or any
#    affiliate of the UC system shall be liable for any damages suffered by
#    Licensee from the use of this software.
#
# $Id: config.in,v 1.32 2001/04/12 18:35:00 jmartin Exp $
# Anything following a "#" is treated as a comment.

##################################################################################

# The folowing parameter represents the maximum simulation time. The numberd
# portion can be followed by optional letters to modify the simulation time.
# For example:
#           100NS   - 100 nano-seconds
#           100MS   - 100 milli-seconds
#           100S    - 100 seconds
#           100     - 100 seconds (default case)
#           100M    - 100 minutes
#           100H    - 100 hours
#           100D    - 100 days

SIMULATION-TIME         1D
#
# The following is a random number seed used to initialize  part of the seed of
# various randomly generated numbers in the simulation. This can be used to vary
# the seed of the simulation to see the consistency of the results of the
# simulation.
#
SEED                    1
```

```
#
# The following two parameters stand for the physical terrain in which the nodes
# are being simulated. For example, the following represents an area of size 100
# meters by 100 meters. All range parameters are in terms of meters.
#
# Terrain Area we are simulating.
#
TERRAIN-DIMENSIONS   (2000, 2000)
#
# The following parameter represents the number of nodes being simulated.
#
NUMBER-OF-NODES        50
#
#The following parameter represents the node placement strategy.
#- RANDOM: Nodes are placed randomly within the physical terrain.
#- UNIFORM: Based on the number of nodes in the simulation, the physical
#  terrain is divided into a number of cells. Within each cell, a node is
#  placed randomly.
#- GRID: Node placement starts at (0, 0) and are placed in grid format with
#  each node GRID-UNIT away from its neighbors. The number of nodes has to be
#  square of an integer.
#- FILE: Position of nodes is read from NODE-PLACEMENT-FILE. On each line of
#  the file, the x and y position of a single node is separated by a space.
#
# NODE-PLACEMENT         FILE
# NODE-PLACEMENT-FILE ./nodes.input
# NODE-PLACEMENT         GRID
# GRID-UNIT                          30
#NODE-PLACEMENT          RANDOM
NODE-PLACEMENT           UNIFORM
#
# The following represent parameters for mobility. If MOBILITY is set to NO,
# than there is no movement of nodes in the model. For the RANDOM-DRUNKEN model,
# if a node is currently at position (x, y), it can possibly move to (x-1, y),
# (x+1, y), (x, y-1), and (x, y+1); as long as the new position is within the
# physical terrain. For random waypoint, a node randomly selects a destination
# from the physical terrain. It moves in the direction of the destination in
# a speed uniformly chosen between MOBILITY-WP-MIN-SPEED and
# MOBILITY-WP-MAX-SPEED (meter/sec). After it reaches its
# destination, the node stays there for MOBILITY-WP-PAUSE time period.
# The MOBILITY-INTERVAL is used in some models that a node updates its position
# every MOBILITY-INTERVAL time period. The MOBILITY-D-UPDATE is used that a node
# updates its position based on the distance (in meters).
#

MOBILITY          NONE

# Random Waypoint and its required parameters.

#MOBILITY RANDOM-WAYPOINT
#MOBILITY-WP-PAUSE                     30S
#MOBILITY-WP-MIN-SPEED            0
#MOBILITY-WP-MAX-SPEED          10

#MOBILITY TRACE
#MOBILITY-TRACE-FILE ./mobility.in
#MOBILITY PATHLOSS-MATRIX
# The following parameters are necessary for all the mobility models

MOBILITY-POSITION-GRANULARITY 0.5
# PROPAGATION-LIMIT:
#   Signals with powers below PROPAGATION-LIMIT (in dBm)
#   are not delivered. This value must be smaller than
#   RADIO-RX-SENSITIVITY + RADIO-ANTENNA-GAIN of any node
#   in the model. Otherwise, simulation results may be
#   incorrect. Lower value should make the simulation more
#   precise, but it also make the execution time longer.
#
PROPAGATION-LIMIT          -111.0
# PROPAGATION-PATHLOSS: pathloss model
#   FREE-SPACE:
#      Friss free space model.
#      (path loss exponent, sigma) = (2.0, 0.0)
#   TWO-RAY:
#      Two ray model. It uses free space path loss
#      (2.0, 0.0) for near sight and plane earth
#      path loss (4.0, 0.0) for far sight. The antenna
#      height is hard-coded in the model (1.5m).
#   PATHLOSS-MATRIX:
#
#PROPAGATION-PATHLOSS    FREE-SPACE
PROPAGATION-PATHLOSS    TWO-RAY
#PROPAGATION-PATHLOSS    PATHLOSS-MATRIX
#
# NOISE-FIGURE: noise figure
#
NOISE-FIGURE      10.0
#
# TEMPARATURE: temparature of the environment (in K)
#
TEMPARATURE       290.0
###############################################
#
# RADIO-TYPE: radio model to transmit and receive packets
#   RADIO-ACCNOISE: standard radio model
#   RADIO-NONOISE: abstract radio model
#   (RADIO-NONOISE is compatible with the current version (2.1b5)
#     of ns-2 radio model)
```

```
RADIO–TYPE                  RADIO–ACCNOISE
#RADIO–TYPE                 RADIO–NONOISE

#
# RADIO–FREQUENCY: frequency (in heltz) (Identifying variable for multiple radios)
RADIO–FREQUENCY       2.4e9
# RADIO–BANDWIDTH: bandwidth (in bits per second)
RADIO–BANDWIDTH       2000000
#
# RADIO–RX–TYPE:  SNR–BOUNDED
# RADIO–RX–SNR–THRESHOLD 10.0
# RADIO–RX–SNR–THRESHOLD 8.49583.
# RADIO–RX–TYPE               BER–BASED
# BER–TABLE–FILE              ./ber_bpsk.in
# RADIO–TX–POWER: radio transmition power (in dBm)
   RADIO–TX–POWER             16.96
# RADIO–ANTENNA–GAIN: antenna gain (in dB)
   RADIO–ANTENNA–GAIN  0.0
# RADIO–RX–SENSITIVITY: sensitivity of the radio (in dBm)
   RADIO–RX–SENSITIVITY  −91.0
# RADIO–RX–THRESHOLD: Minimum power for received packet (in dBm)
    RADIO–RX–THRESHOLD  −81.0

################################
MAC–PROTOCOL               802.11
# MAC–PROTOCOL             CSMA
# MAC–PROTOCOL             MACA
# MAC–PROTOCOL             TSMA
# TSMA–MAX–NODE–DEGREE           8
#MAC–PROPAGATION–DELAY 1000NS
#
# PROMISCUOUS–MODE defaults to YES and is necessary if nodes want
# to overhear packets destined to the neighboring node.
# Currently this option needs to be set to YES only for DSR is selected
# as routing protocol.  Setting it to ”NO” may save a trivial amount
# of time for other protocols.
#PROMISCUOUS–MODE        NO

##############################
# Currently the only choice.

NETWORK–PROTOCOL        IP
NETWORK–OUTPUT–QUEUE–SIZE–PER–PRIORITY  100
# RED–MIN–QUEUE–THRESHOLD  150
# RED–MAX–QUEUE–THRESHOLD  200
# RED–MAX–MARKING–PROBABILITY  0.1
# RED–QUEUE–WEIGHT  .0001
# RED–TYPICAL–PACKET–TRANSMISSION–TIME  64000NS

##############################
#ROUTING–PROTOCOL       BELLMANFORD
#ROUTING–PROTOCOL       AODV
#ROUTING–PROTOCOL       DSR
#ROUTING–PROTOCOL       LAR1
#ROUTING–PROTOCOL       WRP
#ROUTING–PROTOCOL       FISHEYE
ROUTING–PROTOCOL        BTP
#ROUTING–PROTOCOL         DBF
#ROUTING–PROTOCOL       ZRP
#ZONE–RADIUS            2
#ROUTING–PROTOCOL       STATIC
#STATIC–ROUTE–FILE      ROUTES.IN
#
# The following is used to setup applications such as FTP and Telnet.
# The file will need to contain parameters that will be use to
# determine connections and other characteristics of the particular
# application.
#
APP-CONFIG-FILE     ./app.conf
#
# The following parameters determine if you are interested in the statistics of
# a a single or multiple layer. By specifying the following parameters as YES,
# the simulation will provide you with statistics for that particular layer. All
# the statistics are compiled together into a file called "GLOMO.STAT" that is
# produced at the end of the simulation. If you need the statistics for a
# particular node or particular protocol, it is easy to do the filtering. Every
# single line in the file is of the following format:
# Node:      9, Layer:  RadioNoCapture, Total number of collisions is 0
#
APPLICATION-STATISTICS          YES
TCP-STATISTICS                                  YES
UDP-STATISTICS                                  YES
ROUTING-STATISTICS                              YES
NETWORK-LAYER-STATISTICS                YES
MAC-LAYER-STATISTICS                    YES
RADIO-LAYER-STATISTICS                  YES
CHANNEL-LAYER-STATISTICS                YES
MOBILITY-STATISTICS                             NO
# GUI-OPTION: YES allows GloMoSim to communicate with the Java Gui Vis Tool
#             NO does not
GUI-OPTION              NO
GUI-RADIO              NO
GUI-ROUTING            NO
```

Bibliography

[1] P. Narula, S. K. Dhurandher, S. Misra, and I. Woungang., “Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing,” *Computer Communications*, vol. 4, pp. 760–769, March 2008.

[2] N. Roux, J. Pegon, and M. Subbarao, “Cost adaptive mechanism to provide network diversity for MANET reactive routing protocols,” in *Proc. IEEE 21th Military Communications Conference*, (LA, CA, USA.), October 22-25 2000.

[3] N. Garg, K. Aswal, and D. C. Dobhal, “A review of routing protocols in mobile ad hoc networks,” *International Journal of Information Technology and Knowledge Management*, vol. 5, pp. 177–180, Jan-June 2012.

[4] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, “A review of routing protocols for mobile adhoc networks,” *Ad Hoc Networks 2004*, pp. 1–22, 2004.

[5] network working group, “The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4,” 2007. http://tools.ietf.org/html/rfc4728, [Online: accessed 30-Nov-2012].

[6] D. B. Johnson and D. A. Maltzion, “Dynamic source routing in ad hoc wireless networks,” in *Mobile Computing*, pp. 153–181, Kluwer Academic Publishers, 1996.

[7] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An overview of mobile ad hoc networks: Applications and challenges," *Journal of the Communications Network*, vol. 3, pp. 60–66, July 2004.

[8] A. Ephremides, "Energy concerns in wireless networks," *IEEE Wireless Communications*, pp. 48–59, December 15-17 2002.

[9] K. Aniruddha, A. Radhika, and D. Joshi, "Optimization of energy consumption for OLSR routing protocol in MANET," *International Journal of Wireless and Mobile Networks (IJWMN)*, vol. 4, pp. 251–262, February 2012.

[10] S. Suganya and S. Palaniammal, "An optimized energy consumption algorithm for MANET," *International Conference On Modelling Optimization and Computing*, vol. 38, pp. 903–910, 2012.

[11] M. AL-Gabri, L. Chunlin, Y. Zhiyong, A. N. Hasan, and Z. Xiaoqing, "Improved the energy of ad hoc on-demand distance vector routing protocol," *International Conference on Future Computer Supported Education*, vol. 2, p. 355–361, August 22-23 2012.

[12] P.S.Hiremath and S. M.Joshi, "Energy efficient routing protocol with adaptive fuzzy threshold energy for MANETs," *IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC)*, vol. 2, pp. 402–407, June 2012.

[13] S. Rout, A. K. Turuk, and B. Sahoo, "Energy aware routing protocol in MANET using power efficient topology control method," *International Journal of Computer Applications (0975 – 8887)*, vol. 43, pp. 33–42, April 2012.

[14] A. Kumar, M. Q. Rafiq, and K. Bansal, "Energy efficient routing protocol avoiding route breaks based on DSR," *International Journal of Computer Applications (0975 – 8887)*, vol. 44, pp. 39–44, April 2012.

[15] S. Verma, R. Agarwal, and P. Nayak, “An optimized energy aware routing (OEAR) scheme for mobile ad hoc networks using variable transmission range,” *International Journal of Computer Applications (0975 – 8887)*, vol. 45, pp. 18–22, May 2012.

[16] D. K. Anand and S. Prakash, “Design and energy efficient DSDV routing protocol for Mobile Ad Hoc Networks,” *International Journal of Advances in Engineering and Technology (IJAET)*, vol. 5, no. 1, pp. 526–535, 2012.

[17] *Security of e-Systems and Computer Networks.* Cambridge University Press, U.K., 2007. ISBN:9780521837644.

[18] I. Woungang and M. K. Denko, “Credit-based cooperation enforcement schemes tailored to opportunistic networks,” in *Chapter 3: in M. Denko et al. (Eds.), Mobile Opportunistic Networks: Architectures, Protocols and Applications*, ch. 3, Boca Raton, Florida: Auerbach Publications, Taylor and Francis Group, Jan 2011.

[19] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, “Smart: A secure multi-layer credit based incentive scheme for delay-tolerant networks,” *IEEE Transactions on Vehicular Technology*, vol. 58, October 2009.

[20] H. Janzadeh, K. Fayazbakhsh, M. Dehghan, and M. S. Fallah, “A secure credit –based cooperation stimulating mechanism for manets using hash chains,” *In Future Generation Computer Systems*, vol. 25, pp. 926–934, September 2009.

[21] J. Hu and M. Burmester, “LARS: A locally aware reputation system for mobile ad hoc networks,” in *Proc. of 44th Annual Southeast Regional Conference*, (New York, NY, USA), pp. 119–123, 2006.

[22] Y. Hu, A. Perrig, and D. B. Johnson, “ARIADNE: A secure on-demand routing protocol for ad hoc networks,” *Wireless Networks*, vol. 11, p. 21–38, January 2005.

[23] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proceedings of the 10th IEEE International Conference on Network Protocols*, ICNP '02, (Washington, DC, USA), pp. 78–89, November 12-15 2002.

[24] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, 1976. IT-22(6), 644–654.

[25] F. D. Rango and S. Marano, "Trust-based SAODV protocol with intrusion detection and incentive cooperation in MANET," in *Proc. of Intl. Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, (Leipzig, Germany), pp. 1443–1448, 2009.

[26] T. Haniotakis, S. Tragoudas, and C. Kalapodas, "Security enhancement through multiple path transmission in ad hoc networks," in *Proc. of IEEE Intl. Conference on Communications*, (Paris, France), pp. 4187–4191, June 2004.

[27] S. K. Dhurandher and V. Mehra, "Multi-path and message trust-based secure routing in ad hoc networks," in *Proc. of Intl. Conference on Advances in Computing, Control and Telecommunications Technologies*, (India), pp. 189–194, December 28-29 2009.

[28] B. Forouzan, *Data Communication and Networking", 4/e.* McGraw–Hill, 2007. ISBN: 0072967757.

[29] A. Kush and S. Taneja, "Secured routing over manet with power management," in *ACAI '11 Proc. of the International Conference on Advances in Computing and Artificial Intelligence*, (New York, NY, USA), pp. 144–149, ACM, 2011.

[30] Y. Z.-W. Li, Z. Yang, and Z. Chun-Kai, "A power-aware adaptive dynamic routing scheme for wireless ad hoc networks," in *Proc. of the IEEE In-ternational Conference on Networking, Sensing and Control(ICNSC 2008)*, (Sanya, China), pp. 966–970, April 6-8 2008.

[31] S. Singh, M. Woo, and S. Raghavendr, “Power-aware with routing in mobile ad hoc networks,” in *Proc. of ACM/IEEE Intl. Conference on Mo-bile Computing and Networking (MobiCom’98)*, (Dallas, TX, USA), 1998.

[32] S. Kumari and D. M. Shrivastava, “Secure DSR protocol in MANET using energy efficient intrusion detection system,” *International Journal of Networks and Systems*, vol. 1, pp. 6–11, August-September 2012. ISSN 2319-5975.

[33] S. S. Gaikwad, O. S. Rajandar, G. T. Chavan, and S. M. Mate, “Secure power aware routing to support real-time traffic in mobile ad hoc networks,” *Intl. Journal on Cloud Computing: Services and Architecture (IJCCSA)*, vol. 2, February 2012.

[34] J. Chang and L. Tassiulas, “Energy conserving routing in wireless ad hoc networks,” in *Proc. of the 9th IEEE International Conference on Computer Com-munications (INFOCOM 2000)*, (Tel-Aviv, Israel), pp. 22–31, March 26-30 2000.

[35] S. Marti, T. J. Giuli, and K. Lai, “Mitigating routing misbehavior in mobile ad hoc networks,” in *Proceedings of MobiCom 2000*, (Boston, USA), pp. 255–265, August 2000.

[36] L. Sheng, J. Shao, and J. Ding, “A novel energy-efficient approach to dsr based routing protocol for ad hoc network,” in *Proceedings of Intl. Conference on Electrical and Control Engineering*, (Harbin, China), pp. 2618–2620, June 25-27 2010.

[37] R.Vadivel and V. M. Bhaskaran, “Energy efficient with secured reliable routing protocol (eesrrp) for mobile ad-hoc networks,” *Procedia Technology*, pp. 703–707, 2012.

[38] M. R. Babu, “An energy efficient secure authenticated routing protocol for mobile adhoc networks,” *American Journal of Scientific Research*, no. 9, pp. 12–22, 2010. ISSN 1450-223X.

[39] S. Taneja and A. Kush, “Energy efficient, secure and stable routing protocol for MANET,” *Global Journal of Computer Science and Technology, Network, Web and Security*, vol. 12, May 2012. Version 1.0.

[40] R.Vadivel and B. Narasimhan, “A novel energy efficient authentic reliable routing protocol (EEARRP) for scalable mobile ad hoc networks,” *International Journal of Computer Applications (0975 – 8887)*, vol. 56, October 2012.

[41] A. Banerjee, A. Bhattacharyya, and D. Bose, “Power and trust based secured routing approach in MANET,” *International Journal of Security, Privacy and Trust Management (IJSPTM)*, vol. 1, August 2012.

[42] H. N. Saha, D. Bhattacharyya, and P. K. Banerjee, “Energy efficient administrator based secure routing in MANET,” in *Advances in Intelligent Systems and Computing*, vol. 167, (New Delhi, India), pp. 659–672, 2012.

[43] M.Tamilarasi and T.V.P.Sundararajan, “Secure enhancement scheme for detecting selfish nodes in MANET,” in *Proc. of International Conference on Computing, Communication and Applications (ICCCA), 2012*, (Tamilnadu, India), pp. 1–5, February 2012.

[44] R. Vijayan, V. Mareeswari, and K.Ramakrishna, “Energy based trust solution for detecting selfish nodes in MANET using fuzzy logic,” *International Journal of Research and Reviews in Computer Science (IJRRCS)*, vol. 2, pp. 647–652, June 2011.

[45] S.Gopinath, Dr.A.Rajaram, and N. Kumar, “Improving minimum energy consumption in ad hoc networks under different scenarios,” *International Journal of Advanced And Innovative Research (IJAIR)*, pp. 40–46, September 2012. ISSN: 2278-7844.

[46] A. Pirzada and C. McDonald, “Establishing trust in pure ad-hoc networks,” in *Proc. of the 27th Australasian Conference on Computer Science (ACSC’04)*, (Dunedin, New Zealand), pp. 47–54, 2004.

[47] Z. Liu, A. W. Joy, and R. A. Thompson, “A dynamic trust model for mobile ad-hoc networks,” in *Proc. of 10th IEEE Intl. Workshop on Future Trends of Distributed Computing Systems*, (Suzhou, China), pp. 80–85, 26-28 May 2004.

[48] M. G. X. Zeng, R. Bagrodia, “Glomosim: A library for the parallel simulation of large-scale wireless networks,” in *Proc. of the 12th Workshop on Parallel and distributed Simulation*, (Banff, Alberta, Canada), pp. 154–161, May 1998.

[49] R. Bargodia, R. Meyer, M. Takai, Y. Chen, X. Zeng, J. Martin, and H. Y. Song, “PARSEC: A parallel simulation environment for complex systems,” *IEEE Computer*, vol. 31, pp. 77–85, October 1998.

[50] D. Barker, “The OSI network model explained,” *Databases and Network Journal*, vol. 42, p. 3, October 2012.