ENHANCE COMMUNICATION SECURITY IN WIRELESS AD HOC NETWORKS THROUGH MULTIPATH ROUTING

By

LI ZHAO

A dissertation submitted in partial fulfillment of
the requirements for the degree of

DOCTOR OF PHILOSOPHY

WASHINGTON STATE UNIVERSITY
School of Electrical Engineering and Computer Science

AUGUST 2007

To the Faculty of Washington State University:

The members of the Committee appointed to examine the dissertation of LI ZHAO find it satisfactory and recommend that it be accepted.

_____
Chair

_____

_____

Acknowledgements

My first, and most earnest, acknowledgment must go to my advisor Dr. José G. Delgado-Frias for his continuous encouragement, advice, mentoring, inspiration, and research and financial support throughout my Ph.D. study. Dr. Delgado was always there to listen and give advice. I appreciate his patience and numerous help during the last few years.

I would like to thank the rest members of the doctoral committee: Dr. Jabulani Nyathi, for his friendship, encouragement, and insightful suggestions, and Dr. Krishnamoorthy Sivakumar, who shared his research ideas and showed great support to my dissertation and defense.

I am greatly indebted to my first advisor at Washington State University, Dr. Krishna Sivalingam. He helped me start my journey to become a Ph.D., gave me academic and financial support and advice, and encouraged me throughout my first year here. I would also like to thank Dr. Ben Belzer for sharing his academic experience and giving helpful advice.

During the course of this work at Washington State University, I was partly supported by the EECS as Teaching Assistant. All opinions expressed in this work are the author's and do not necessarily reflect the policies and views of EECS and WSU.

Finally, I would like to convey special gratitude to my family: my parents and my sister. I thank them for their unconditional love, understanding, support, patience, and believe in me over

the last few years. It would be impossible to have my research career without them standing behind me. This dissertation is dedicated to them. I also thank my friends for their encouragement and support.

To all of you, thank you!

ENHANCE COMMUNICATION SECURITY IN WIRELESS AD HOC NETWORKS THROUGH MULTIPATH ROUTING

Abstract

by Li Zhao, Ph.D.
Washington State University
August 2007

Chair: José G. Delgado-Frias

The specific characteristics of Mobile Ad Hoc Networks (MANETs) make cooperation among all nodes and secure transmission important issues in its research. A number of research studies using single path or multipath transmission to safeguard communication against intermediate node misbehavior have been conducted. In this dissertation, we propose and evaluate a novel secure scheme, MultipAth Routing Single- path transmission (MARS), to secure data transmission in ad hoc networks. The MARS scheme is proposed from the cross-layer perspective. Multipath routing, single path data transmission, and end-to-end feedback mechanism are combined to provide better network performance and more comprehensive protection against misbehavior on data formed by individual or colluding misbehaving nodes. The MARS scheme, its enhancement E-MARS, the secure transmission protocol TWOACK, and the DSR protocol are evaluated by means of simulation under various adverse scenarios. The simulation results show that the MARS and E-MARS provide considerable protection to ad hoc networks at the expense of moderate overhead. In a network with 20% misbehaving nodes, the MARS and E-MARS have up to 45% higher data receive rate than the DSR under individual

misbehavior. The data receive rates of MARS and E-MARS are higher up to 50% and 28% respectively under individual or colluded misbehavior with 40% misbehaving nodes in the network.

To compare our protocols with multipath secure schemes, we also assess the impact of interactions between MAC-layer protocols and data forwarding along network-layer paths on multipath data transmission over multihop IEEE 802.11 MAC-based wireless networks. The frame service time at source in 802.11 MAC-based multipath data transmission system under unsaturated conditions is studied. Analytical models have been developed for two packet generation schemes (round robin and batch) with Poisson frame arrival process. Moreover, an analytical model is used to investigate the throughput of multipath transmission system in 802.11-based multihop wireless networks. Two methods have been developed to estimate the impact of cross-layer interactions on the frame service time in such a system. Two bounds of the system throughput are obtained based on these estimation methods. These models are validated by means of simulation under various scenarios.

Contents

List of Tables

List of Figures

Dedication

My Parents

Chapter 1

Introduction

Recent advances in wireless technologies have made possible of the design of novel wireless devices, including cellular phones, laptops, personal digital assistants (PDAs), and micro-sensors. These technologies have enabled the development of mobile ad hoc networks (MANETs), in which different types of mobile nodes with different goals share their resources in a network-wide area. The operation of MANETs does not depend on pre-existing infrastructure or base stations. A node is able to communicate with another node within its range through other nodes if the destination node is not in the immediate neighborhood. However, there may be misbehaving nodes that can rather easily disrupt the network operation and damage the communication within the network area. Hence, providing secure data communication through misbehavior detection and mitigation in MANETs is an important and critical research topic. In this dissertation this problem is investigated and novel solutions are proposed and evaluated to maintain a level of performance of MANETs with misbehaving nodes. In this chapter, an introduction and background for the proposed solutions are provided. The organization of this chapter is as follows. An overview of ad hoc networks and ad hoc network security is provided in Sections 1.1 and 1.2. The IEEE 802.11 MAC protocols, routing in MANETs, and multipath transmission system in wireless networks are introduced in Sections 1.3, 1.4, and 1.5. Finally, the

problem statement is stated in Section 1.6 and the organization of this dissertation is provided in Section 1.7.

1.1 Overview of Ad Hoc Networks

There are two types of wireless mobile networks at present. These networks can be categorized into two architecture classes with different operation mechanisms and related issues.

One type is *infrastructured* wireless networks, in which there are fixed wireless gateways that connect the mobile systems with a wired network. Typical applications of such networks are the cellular phone networks and the wireless local area networks (WLANs). The gateways in the cellular phone systems are known as base stations, and the infrastructure in a WLAN are called the access points (APs). The networks with infrastructure are suitable for locations where base stations are present or can be easily placed. An advantage of this type of networks is that the existing wired networks can be employed to support access from mobile users without modifications to the networks' control structure. A disadvantage of these networks is that the fixed infrastructure would constrain node mobility, limit network deployability, and increase installation and management costs of the networks.

In a place where infrastructure cannot be placed or not currently available, another type of mobile wireless networks, commonly known as *mobile ad hoc networks* (MANETs), are employed. A MANET consists of a collection of mobile nodes which communicate with each other via wireless links in a self-organized way without fixed network infrastructure and any centralized administration. Nodes in an ad hoc network operate equally and are free to move randomly. Therefore, the network topology may change rapidly and unpredictably. As each individual node in the network has limited wireless transmission range, all network activities, such as discovering network topology and delivering data packets, have to be executed by the

nodes themselves individually and/or collectively. Each node needs to act as a router to forward control and data packets for other nodes. Depending on its application, the structure of an ad hoc network may vary from a highly power-constrained small static network, which is as the case for a sensor network, to a large-scale highly dynamic network.

There are generally two types of MANETs: *closed* and *open* [62]. In a closed MANET, all mobile nodes cooperate with each other toward a common goal, such as emergency search/rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. No matter which type of MANETs is used, an ad hoc network can work properly only if the participating nodes cooperate in a proper way.

The ad hoc networks have been studied in the past in to the context of defense, often under the name of packet radio networks [45]. Recently there has been a renewed interest in this field due to the availability of low-cost laptops and palmtops with radio interfaces. A MANET working group [58] has been formed within the Internet Engineering Task Force (IETF) to develop a framework for ad hoc networks. Some examples of possible applications of ad hoc networks include mobile computer users gathering for a conference, emergency disaster relief personnel coordinating efforts, personal area network (PAN) with wireless devices that are closely associated with a single person and interactions between several PANs when people meet, wireless sensor networks in certain dangerous area, and soldiers relaying information for situational awareness on the battlefield.

1.2 Ad Hoc Network Security

Since there is no administrative facility and central entity in a mobile ad hoc network, the nodes need to collaboratively support all the network activities. To provide reliable communication

service under adversarial environments, securing the basic network operation becomes one of the primary concerns in MANETs. This section describes the main types of misbehavior that can be formed in an ad hoc network.

1.2.1 Communication Phase

Communication in ad hoc networks consists of two phases, *route discovery* and *data transmission*. Under adversarial environments, misbehaving nodes could disrupt the route discovery by obstructing the propagation of legitimate route control traffic and adversely influencing the topological knowledge of benign nodes. Misbehaving nodes could also disrupt the data transmission phase. First, they could abide the route discovery to place themselves on utilized paths. Then, they could tamper with the in-transit data in an arbitrary manner and degrade the network operation. The upper layer mechanisms and the current ad hoc network routing protocols cannot deal with malicious disruptions of data transmission.

1.2.2 Misbehaving Node

In the MANETs, different misbehaving nodes form misbehavior with different purposes. There are generally two types of misbehaving nodes in an ad hoc network. They form misbehavior with different capabilities and out of different purposes.

Malicious nodes, also called attackers, are capable of discarding or altering control and data packets, preventing route discovery between two nodes, make data packets unable to arrive at their destinations while consuming energy and available bandwidth of the network [14, 37]. These nodes are controlled by adversaries. They have the potential to cause harm to the entire network and all types of network operation.

Selfish nodes, which are part of an ad hoc network, use this network to establish their own communication. But they refuse to spend their power for operations that do not directly

benefit them. Selfish nodes can drop data packets or refuse to forward routing control packets for other nodes. Although they are not intended to damage the network, their behavior disturbs the performance and influences the operation of the whole network.

1.2.3 Security Mechanism

Due to its absence of infrastructure, the consequent absence of authorization facilities, and the distributed environment, the traditional security mechanisms (which mostly are depend on encryption and authorization) may not be fully applicable to a MANET. It is difficult to make the mobile nodes establish long-lasting trust relationship with each and every peer they are transiently associated with. This impedes providing cryptographic protection and authentication to all control and data traffic in the network. Moreover, even if this type of services were possible, the associated overhead and delay would pose a challenge in such a dynamic environment. These services cannot be effective against the denial of service (DoS) attack, in which the misbehaving nodes just drop its received data packets. Thus, security schemes specific to the ad hoc environment need to be investigated.

It is a great challenge to secure communication and maintain connectivity in the presence of misbehaving nodes across an unknown and frequently changing multihop wireless network topology as in MANETs. The literature contains a large number of studies on guarding the routing mechanisms against a range of attacks under different assumptions and system requirements in ad hoc networks [37, 38, 39].

Secure routing procedure alone cannot guarantee secure and undisrupted data delivery across the network. Many studies on detecting the misbehavior on data and mitigating the adverse effects to provide secure data transmission in ad hoc networks have been conducted [56]. The proposed work in this dissertation focuses on securing data transmission phase. We present a review about the related work on providing security in ad hoc networks in Chapter 2.

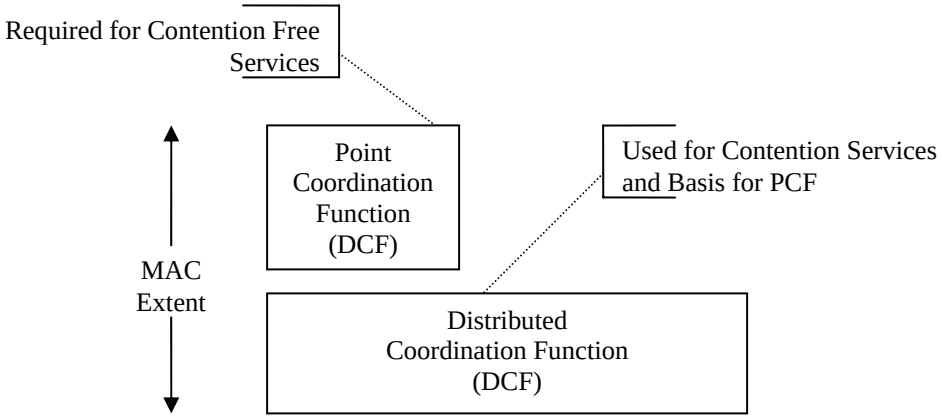


Figure 1.1: IEEE 802.11 MAC architecture.

1.3 Overview of IEEE 802.11

The IEEE 802.11 [41] standard is recommended by IEEE Project 802. The standard provides detailed physical layer (PHY) and medium access control (MAC) specifications for wireless local area networks (WLANs). The IEEE 802.11 MAC has become ubiquitous and gained widespread popularity as a *de facto* layer-2 standard for wireless networks. In this section, a brief description of the core functions of 802.11 MAC is provided.

Currently, the IEEE 802.11 standards include a basic medium access protocol *Distributed Coordination Function* (DCF) and an optional *Point Coordination Function* (PCF). The basic IEEE 802.11 MAC architecture is shown in Figure 1.1 [41]. The PCF is a centralize-scheduling and polling-based protocol, which is designed to support collision free and transmission of real time traffic in wireless networks. The multihop or single-hop ad hoc operation is supported by the DCF, which is based on the Carrier Sense Medium Access with Collision Avoidance (CSMA/CA) random access scheme, in which retransmission of collided packets is managed according to binary exponential backoff rules. In this work, the study is based on DCF scheme.

The DCF uses two techniques for packet transmission. The default scheme, known as basic access method, is a two-way handshaking mechanism. A positive MAC acknowledgement (ACK) is sent out by the destination station upon successful reception of a packet transmitted by the source station. The other optional scheme is a four-way handshaking mechanism, which uses request-to-send/clear-to-send (RTS/CTS) technique to reserve the channel before data transmission. This technique has been introduced to reduce the performance degradation due to hidden terminals. However, the drawback of using the RTS/CTS mechanism is the increase overhead for short data frames. Due to the factors like channel contention delays and collisions in DCF, the performance of the MAC protocol has significant impact on the performance of 802.11-based mobile ad hoc networks. This dissertation concentrates on studying the performance of RTS/CTS technique in IEEE 802.11 DCF.

This dissertation focuses on analyzing the performance of IEEE 802.11 with respect of the interactions between MAC layer protocols and data forward along paths at network layer. We present a review about the related work on IEEE 802.11 in Chapter 2. The proposed scheme and its performance analysis are presented in Chapter 3.

1.4 Routing in MANETs

The characteristics of multihop wireless links, absence of fixed infrastructure, and frequent host mobility present several challenges for MANETs. Among these challenges is routing. The routing protocol must be able to keep up with the high degree of node mobility that often changes network topology drastically and unpredictably. From the perspective of path searching, proposed solutions for routing in MANETs are usually classified into: table-driven, on-demand, hierarchical, power-aware, geographical, and multicast protocols. From the perspective of searching goals, proposed routing solutions are classified into: single-path and multipath.

1.4.1 Single-path Routing

Most of the first proposed routing protocols in MANETs are aimed at the most feasible (primary) path from between two nodes. Some of the better known proposed single-path routing protocols are Destination Sequence Distance Vector routing protocol (DSDV) [68], Ad hoc On-demand Distance Vector (AODV) routing [69], Dynamic Source Routing (DSR) [13], Temporary Ordered Routing Algorithm (TORA) [67], and Location-Aided Routing (LAR) [49].

1.4.2 Multipath Routing

Multipath routing protocols are proposed based on the principle that higher performance can be achieved by recording more than one feasible path. Multipath routing has been explored in several different contexts.

Traditional wired networks use alternate path routing to decrease blocking probability and increase overall network utilization. In alternate path routing, a set of paths, which consist of a primary path and one or more alternate paths, is established between a pair of end nodes. When the primary path for a particular source destination pair becomes unavailable, rather than blocking a connection, an alternate path is deployed. Well known alternate path routing schemes are Dynamic Nonhierarchical Routing [2] and Dynamic Alternative Routing [31].

In MANETs, multiple paths are discovered for other compelling reasons, including lower delay, increased fault tolerance, lower power consumption, load balancing, and higher security. Node mobility in ad hoc networks leads to frequent link breaks. This results in periodic route request broadcasts, consequently higher routing overhead, and route establishment delay. With both data and control packets competing for the same channel, packet delivery is substantially reduced. By implementing multipath routing, data forwarding can continue uninterrupted on other available paths without waiting for finding a new route even if the primary path fails data.

The potential multi-connectivity between neighbor nodes in the MANETs makes the multiple paths between two nodes possible. Multiple paths can be found and used as backups in some single path routing protocols [13, 67]. There are also many on-demand routing algorithms [57, 74, 90] focusing on searching multiple paths in ad hoc networks. It has been proven that the multipath routing algorithms can make nodes get more information about the network topology [22, 51]. This helps the source to find more fresh paths to the destination and improves the data delivery performance. In this study, we use multipath routing to get node-disjointed path between the source and destination.

1.5 Multipath Data Transmission

Multipath data transmission (MDT) in MANETs is the combination of multipath routing and Multiple Description Coding (MDC). It has been studied to provide load balance, support real-time and multimedia applications, and secure data transmission in mobile ad hoc networks [33, 36, 48, 59, 70, 71, 89].

In MDT, a set of L paths (preferably node-disjoint) are established between the source and destination. Each path set are with a set of parameters in terms of bandwidth, delay, loss probabilities, data receive rate, and so on. The transport layer or a specified mechanism [33, 48] is employed to monitor the path parameters and returns such information to the source. At the source, each outgoing message is encoded into a number of pieces based on specific algorithm [71] by introducing redundancy and dispersed among the L paths. At the destination, packets arriving from all the paths are put into a re-sequencing buffer. Some or all the packets assigned to a path may be lost or overdue. Limited retransmission of lost packets may or may not be invoked, depending on the encoding schemes and the end-to-end delay constraint. The decoder at the destination will attempt to reconstruct the original message from the received packets.

Studies in this area have focused on developing routing algorithms searching multiple node-disjoint paths [90] and coding schemes for multipath transmission and frame recovery [33].

Some simulation and analytical studies [25, 81, 89] have investigated the impact of background traffic and node mobility on the performance of multipath transmission system in 802.11-based ad hoc networks. However, these studies do not consider the effect of MAC layer protocols. In our research, we propose a more comprehensive performance analysis of multipath transmission in multihop 802.11 MAC-based wireless ad hoc networks from the perspective of interactions between MAC layer protocol and IP layer data forwarding. The details of our models are presented in Chapter 3.

1.6 The Problem Statement

In this dissertation, we address the problem of detecting misbehavior on data transmission in a mobile ad hoc network and mitigating the adverse effects of the misbehavior. The misbehavior on data formed by both malicious nodes and selfish nodes is considered. The misbehavior can be formed in individual or cooperative bases.

We investigate the impact of interactions between MAC and network layer protocols on the data transmission system. We build and validate analysis models of multipath data transmission system in 802.11-based ad hoc networks from the aspect of such interactions. The analysis models show that single-path data transmission provides better system performance than multipath data transmission in 802.11-based MANETs. Based on the proposed analysis models, we then propose and enhance a novel data transmission security scheme, **M**ultip**A**th **R**outing **S**ingle path transmission (MARS). MARS combines multipath routing and single path data transmission with end-to-end feedback mechanism. In this scheme, the security of data transmission is achieved without restrictive assumptions on the network nodes' trust and network

membership, without the use of intrusion detection schemes, and at the expense of moderate multipath routing overhead only. As MARS employs single path data transmission, it is compared with Dynamic Source Routing (DSR) [13] based secure and non-secure single path transmission systems via simulations under adversarial environments. The simulation results show that the MARS provides better network performance and detects and mitigates various types of misbehavior on data transmission at the expense of moderate overhead. The network remains efficient and effective even under very highly adversarial environments.

1.7 Dissertation Organization

The remainder of this dissertation is organized as follows. Chapter 2 begins by providing a review of ad hoc network security protocols and existing secure data transmission schemes. Drawbacks and unaddressed issues of existing work are identified to provide context to our proposed schemes. This chapter also presents different methods used to analyze the performance of IEEE 802.11 MAC protocols under various network environments. Chapter 3 presents the analysis models at source for IEEE 802.11-based multipath transmission system under unsaturated conditions. It also presents the throughput analysis model of an IEEE 802.11-based multipath multihop ad hoc transmission system. The impact of MAC protocols on multipath data transmission is shown for various scenarios. Chapter 4 describes how our proposed schemes can efficiently detect various types of misbehavior on data and mitigate the adverse effects under adversarial environments. Chapter 5 presents a comprehensive simulation study on the proposed schemes with their comparison to DSR-based secure and non-secure schemes to demonstrate their efficiency. Finally, Chapter 6 gives some concluding remarks and summarizes the contributions of this research.

Chapter 2

Background

This chapter provides background information on topics related to the research conducted in this dissertation. In Section 2.1, different types of security schemes in ad hoc networks are described. Various performance analysis models and methods for IEEE 802.11 MAC protocols are presented in Section 2.2. In Section 2.3, the routing protocols and transmission schemes in wireless mobile ad hoc networks are described, in particular multipath routing protocols and multipath data transmission that related to the proposed schemes and models. In Section 2.4, we summarize the discussion in this chapter.

2.1 Ad Hoc Network Security

The security schemes for mobile ad hoc networks can be classified into different groups from different perspective of analysis. In this section, we discuss the existing security protocols according to their operation mechanism, transmission mechanism, type of aimed misbehavior, and misbehavior detection mechanism.

2.1.1 Proactive vs. Reactive

From the perspective of their operation mechanism, security schemes for MANETs can be divided into two categories: *proactive* and *reactive*. Proactive security schemes try to prevent malicious nodes from launching attacks and encourage selfish nodes to cooperate with other nodes. Reactive mechanisms attempt to detect misbehavior formed in the network, mitigate the adverse effects, punish detected misbehaving nodes, and isolate them from the future network operation in a period of time. This type of protocols mainly focuses on the data transmission procedure to guarantee the network performance.

1. Proactive: to prevent the malicious nodes from forming attacks through changing the contents of packets, security information among mobile nodes is encrypted and authenticated. Some work focuses on protecting the routing procedure to guarantee the success and correctness of established paths between different nodes. A survey of possible threats to the routing protocols and some strategies to address these problems are presented in [85]. Typical examples of such schemes are Secure Efficient Distance vector (SEAD) [38] and Ariadne [39]. One-way hash functions employed in SEAD and a hash tree chain mechanism and various authentication mechanisms [40] are proposed to secure distance vector and path vector routing procedures in mobile ad hoc networks. Ariadne employs efficient symmetric cryptographic primitives to guard the on-demand routing procedure against attacks from malicious nodes. Secure Routing Protocol (SRP) [72] utilizes random keys in each routing request packet to mitigate the detrimental effects of malicious behavior and prevent fabricated, compromised, or replayed route replies during the on-demand routing procedures. The main problem with these authorization systems is the distribution of the authorization information within a dynamically changing network.

To encourage the cooperation among the mobile nodes and prevent selfish behavior during data transmission in mobile ad hoc network, *credit-based* schemes are proposed to

provide incentives for nodes to faithfully perform networking functions. In order to achieve this goal, virtual (electronic) currency or similar payment system may be set up. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services. Two typical examples of credits utilized are the *nuggets* (also called *beans*) [16] and the *nuglet counter* [17]. In the Packet Purse and Trade Models, the sender puts a certain number of nuggets on the data packet to be sent. The packet is dropped if it exhausts its nuggets before reaching the destination. Each intermediate node earns some nuggets for providing the forwarding service. The nuglet counter in a node is decreased when the node sends packets of its own, but increased when it forwards packets for the other nodes. The counter should be positive before a node is allowed to send its packet. The main problem with credit-based schemes is that they usually require some kind of tamper-resistant hardware and/or extra protection for the virtual currency or the payment system.

2. Reactive: most of the reactive protocols are *reputation-based*. In such protocols, network nodes collectively detect and declare the misbehavior of suspicious nodes. Such a declaration is then propagated throughout the network, so that the misbehaving node will be cut off from the rest of the network. Typical examples of security schemes in this class are the scheme in [61] and CONFIDANT protocol in [15]. Two major modules, termed watchdog and pathrater, are combined [61] to detect misbehavior on data transmission, identify and isolate misbehaving nodes, and improve throughput in an ad hoc network. The watchdog module maintains a buffer of recently sent packets and overhears the medium to check whether the next-hop node faithfully forwards the packet. A data packet is cleared from the buffer when the watchdog overhears it being forwarded by the next-hop node over the medium. The watchdog accuses the neighbor to be misbehaving if a data packet remains in the buffer for too long. Based on watchdog's accusations, the pathrater module rates every path and chooses the best path. The CONFIDANT protocol is based on selective altruism and utilitarianism, thus making misbehavior unattractive.

It consists of four important components: monitor, reputation system, path manager, and trust manager. They perform the vital functions of neighborhood watching, node rating, path rating, and sending and receiving alarms, respectively. The behavior of next-hop neighbor is monitored.

There are also reactive schemes protecting on-demand routing procedure in mobile ad hoc networks. One example is the scheme proposed in [24]. It uses one more path to the intermediate node that reply the RREQ message in AODV routing protocol to check whether the path from the intermediate node to the destination node exists or not to detect and fight against the "black hole" attack in an ad hoc network.

In our research, we focus on secure data transmission in mobile ad hoc networks reactively. The following reviewed literatures are mainly reactive protocols.

2.1.2 Multipath vs. Single-path

From the aspect of their transmission mechanism, security schemes of MANETs can be divided into two categorizes: *single-path* transmission and *multipath* transmission. Generally, data packets are transmitted through one path from source to destination in ad hoc networks. To efficiently protect data transmission in mobile ad hoc networks, some security schemes implement multipath data transmission instead of single-path data transmission.

1. Single-path Transmission: security schemes implementing single-path transmission is the majority in the security family. In the single-path schemes, the source and intermediate nodes detect and declare the misbehavior of other nodes individually or collectively. The declaration is propagated throughout the network and the declared misbehaving nodes are avoided in all future paths within a period of time. The single-path schemes are efficient in detecting some types of misbehavior formed individually. Most of them fail to detect misbehavior formed by cooperating nodes. Some typical single-path secure schemes are: watchdog and pathrater [61], TWOACK [4], and 2ACK [24].

In the 2ACK and its early version TWOACK/S-TWOACK, a node sends a special ACK to the node two hops back along the path upon receiving a data packet successfully. This special ACK indicates the forwarding of packet at the intermediate node between these two nodes. Such ACK transmission takes place for all data packets in TWOACK and for a fraction of data packets in 2ACK and S-TWOACK.

2. Multipath Transmission: in the multipath security schemes, the multipath data transmission mechanism, which has been described in Chapter 1, is employed for data communications between the sources and the destinations. Through sending data packets of a frame into L node-disjoint paths at source and re-constructing the frame from received M ($M < L$) or L packets at destination, the adverse effect of misbehavior on data along one single path is mitigated. In multipath schemes, multiple node-disjoint paths between end-nodes are required.

The thought of using multipath transmission to defend routing against denial-of-service (DOS) attacks is proposed in [99]. Recently, studies using multiple node-disjoint paths between the source and destination have been conducted on tackling individual misbehavior and some types of colluded misbehavior. These schemes are able to provide security on data transmission, mitigating the effects of misbehaving nodes, protect secret messages from being compromised by colluded attack, and prevent silent enemy nodes from interception all of the data packets and decoding them to obtain the original frame. Some typical security schemes employing multipath data transmission are: SMT [71], SPREAD [57], the encryption method in [78], and APSL [48].

In the Secure Message Transmission (SMT) scheme, a special ACK packet for each received data packet is sent from the destination back to the source. If not enough data packets for frame reconstruction are received by the destination, the source retransmits the lost data packets through valid paths. SMT aims at mitigating the effect of DOS attack. In SPREAD, the encrypted frame is divided into several packets, which are transmitted through different paths. This can prevent colluded enemy nodes from getting enough information to decode the secret

message. The encryption method proposed in [78] can be used with SPREAD to further protect the transmitted message from being decoded. The Adaptive Path Selection and Loading (APSL) scheme enhances the misbehavior resilience by adaptively loading Reed-Solomon (RS) coded data into multiple node-disjoint paths. It maximizes packet delivery ratio by loading paths according to path state information.

The schemes proposed in our research are different from the above mentioned schemes at that they are single-path transmission systems based on multipath routing algorithms. These secure schemes would detect and mitigate effects of misbehavior formed by both individual and colluded misbehaving nodes.

2.1.3 Individual vs. Colluded

There are two types of misbehaving nodes exist in a mobile ad hoc network: *selfish* nodes and *malicious* nodes. Out of the intention of saving their own resources, selfish nodes refuse to service for other nodes. They form misbehavior individually. Malicious nodes intrude into the network with more resources. They can work individually or collaboratively to cause as much damage to the network operation as they can. Hence, the security schemes can also be classified into two categories as against: *individually* and *cooperating* formed misbehaver.

1. Individual Misbehavior: most of the security schemes can defend against misbehavior formed by individual node. Some of the schemes, such as TWOACK, 2ACK, and watchdog and pathrater, aim at detecting misbehavior from individual selfish nodes in the network. Other secure schemes, such as Aidane, are intended to detect misbehavior from individual malicious nodes and isolate these nodes from the network. All the schemes discussed in this Chapter can tackle individual misbehavior. Hence, they are not re-listed again at this subsection.

2. Colluded Misbehavior: By now, there are relatively few proposed schemes tackling misbehavior conducted by two or more cooperating nodes. As colluding malicious nodes are

capable of forming a variety of colluded misbehavior to disrupt or damage the communication in mobile ad hoc networks, generally one scheme is designed to protect network against one specified type of colluded misbehavior.

One chance of forming colluded misbehavior is two or more colluding malicious nodes connected along one data transmission path. These malicious nodes put themselves in very powerful positions to cause damage to the data communications, such as dropping, modifying, compromising, and decoding data packets. One type of such colluded misbehavior is the wormhole attack, which is formed by two connected and cooperating malicious nodes to disrupt network routing by short-circuiting the normal flow of routing control packets. To detect and thus defend against wormhole attack, a notion of *packet leash* is introduced in [37]. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Two types of leash, geographical leash and temporal leash, are discussed. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance. Either types of leash can prevent the wormhole attack, as it allows the receiver of a packet to detect if the packet traveled further than the leash allows.

To provide protection to secret messages from being compromised when they are delivered across the insecure network, Security Protocol for Reliable dAta Delivery (SPREAD) is presented in [57]. The colluded misbehavior aimed at by this scheme is at least one compromised node is located on each of the node-disjoint paths selected to deliver the message. The basic idea of the SPREAD is to transmit a secret message through multipath transmission system so that even if a small number of nodes that are used to repay the message shares are compromised, the secret message as a whole is not compromised. The encrypt schemes in [78] also protect data transmission in sensor networks against such type of colluded attacks. For the security in routing procedures, a technique in [75] identifies and defends multiple cooperating black hole nodes.

The proposed schemes in our research provide protection to data transmission in mobile ad hoc networks against both individual and colluded misbehaving formed by selfish and malicious nodes efficiently. The type of colluded misbehavior considered here is formed by cooperating malicious nodes that are connected with each other along the selected path for data transmission.

2.1.4 Overhearing vs. Acknowledgment

Due to the characteristics of wireless transmission channel, a data transmission at a node can be sensed by all its neighbor nodes. Some schemes use this feature to detect misbehavior or misbehaving nodes by making each node monitor the behavior of its neighbors by *overhear*ing transmission within its radio range area. There are other schemes that use *acknowledgements* to detect misbehavior or malicious nodes in wireless networks.

1. Overhearing: in this type of schemes, the nodes use promiscuous mode of link layer to observe misbehavior of neighborhood nodes. Some typical schemes that detect misbehavior through overhearing mechanism in wireless networks are: the Context Aware detection discussed in [73] and the watchdog module presented in [61]. The Context Aware scheme uses *un-keyed hash chains* and promiscuous mode to detect the misbehavior during route searching procedure. The observers of misbehavior independently communicate their accusation to the source. The source executes an inference scheme based on majority voting to rate an accused, and later on advertise these rating along with adequate proofs to trusted nodes. Different with the Context Aware scheme, the watchdog module monitors the behavior of neighbor nodes during the data forwarding procedure, and in [61] a pathrater is employed to evaluate the performance of nodes along data transmission paths and notify system of detected misbehavior.

2. Acknowledgement: there are several schemes employing different types of acknowledgements (ACKs) to detect misbehavior in ad hoc networks. In order to identify malicious nodes forming black-hole attacks, in which the nodes draw traffic towards themselves

but fail to correctly forward the traffic, the *secure traceroute* protocol was presented in [66]. The source sends packets with increasing Time-To-Live (TTL) value and waits for a warning message from the router at which time the packet's TTL value expires. The traceroute packets are authenticated and disguised as regular data packets. In the 2ACK [56] and its early version TWOACK/S-TWOACK [4], a node sends a special ACK to the node two hops back along the path upon receiving a data packet successfully. The BFTR [94] and SMT [71] schemes use end-to-end acknowledgements (ACKs) for each received data packet to help the source monitor the quality of paths in use. The BFTR employs single-path transmission system. Through end-to-end ACK for each data packet, the BFTR scheme continuously monitors the quality of the path in use. If the behavior of the route deviates from the predefined expected behavior of good paths, it is marked as "infeasible" and a new route is used. Since BFTR throws out the entire path before detecting the misbehaving nodes, the newly chosen path may still include the same misbehaving nodes. Multiple node-disjoint paths are used for data transmission in SMT scheme. If the source could not receive the ACK for a packet transmitted through one path within a timeout limit, it would remove the path from the active path set (APS) and switch data transmission to another path in the APS. The same misbehaving node would not be included in the newly selected path. These repeated ACKs for data packets increase the overhead of data transmission.

The overhearing schemes [73, 61] and some of the ACK schemes [66, 56] can effectively detect the data dropping misbehavior. However, these schemes do not have enough mechanism to detect data modification by the malicious nodes during data transmission. The scheme proposed in [94] can detect and mitigate the data modifying misbehavior.

A different notification system is employed in the security schemes proposed in this work. In our schemes, the destination is responsible of detecting misbehaving path and a notification packet is sent back to the source only when the selected path is deemed to be infeasible. These schemes can detect data modifying misbehavior as well as data dropping misbehavior efficiently.

2.1.5 Discussion

Although the existing research on ad hoc network security has explored many methodologies, there has been no strategy perfect for all adverse scenarios. Tradeoffs between many factors, e.g. efficiency, energy saved, control overhead, and network performance in terms of network throughput, packet delay, etc., have been considered in the literature. In Chapter 4, two novel security schemes for mobile ad hoc networks are presented.

2.2 IEEE 802.11 DCF

The DCF in IEEE 802.11 MAC protocol is the *de facto* standard for mobile ad hoc networks. The efficiency of the 802.11 DCF directly affects utilization of channel capacity and system performance. Performance of the DCF has been studied experimentally and analytically under *saturated* and *unsaturated* conditions for *single-hop* and *multihop* scenarios. The performance is also studied from the *cross-layer* perspective. The performance metrics examined generally are: throughput, delay, power consumption, and scalability. In this section, we will discuss the 802.11 DCF and the work analyzing its performance under various conditions in detail.

2.2.1 IEEE 802.11 DCF

In 802.11 DCF protocols, when a station has new packets to transmit, it persists to monitor the channel until the channel is measured idle for a period of time equal to a distributed interframe space (DIFS). To minimize the probability of collision with packets from other stations, the station then generates a random backoff interval before transmitting. To avoid channel capture, a station also needs to wait a random backoff time between two consecutive transmissions even if the medium is sensed idle in the DIFS time.

Table 2.1: Slot time, minimum and maximum contention window values for the three PHY specified by the 802.11 standard.

PHY	Slot Time (σ)	CW_{min}	CW_{max}
FHSS	50μs	16	1024
DSSS	20μs	32	1024
IR	8μs	64	1024

DCF employs a *discrete-time scale* for efficiency. The time immediately following an idle DIFS is slotted, and a station is allowed to transmit only at the beginning of each slot time. The slot time size σ, as shown in Table 2.1, is set to the time needed at any station to detect the transmission of a packet from any other stations. It depends on the physical layer and accounts for the propagation delay, the time needed to switch from the receiving to the transmitting state, and the time to signal to the MAC layer the state of the channel.

DCF adopts an *exponential backoff* scheme. At each transmission, the backoff time is uniformly chosen in the range (0, $w - 1$), where w is called contention window and depends on the number of transmissions failed for the packet. At the first transmission attempt, w is set equal to a value CW_{min}, called minimum contention window. After each unsuccessful transmission, w is doubled, up to a maximum value $CW_{max} = 2^m CW_{min}$. The values CW_{min} and CW_{max} reported in the final version of the standard [41] for three PHY-specific schemes are summarized in Table 2.1. The backoff time counter is decremented as long as the channel is sensed idle, "frozen" when a transmission is detected on the channel, and reactivated when the channel is sensed idle again for more than a DIFS. The station transmits when the backoff time reaches zero.

The DCF describes two techniques for packet transmission. The basic one is *two-way handshaking* access mechanism. To signal the successful packet reception, an ACK is transmitted by the destination station after a period of time called short interframe space (SIFS).

SIFS is shorter than a DIFS so that no other station is able to claim an idle channel at the end of ACK. If the transmitting station does not receive the ACK within a specified timeout or detects the transmission of a different packet on the channel, it reschedules the packet transmission according to the backoff rules.

The other access mechanism defined in DCF is *four-way handshaking* technique, known with the name RTS/CTS, as shown in Figure 2.1. A station with packets waits until the channel is sensed idle for a DIFS, follows the backoff rules explained above, and transmits a special short frame called request to send (RTS) instead of the packet. When the receiving station detects an RTS frame, it responds, after a SIFS, with a clear to send (CTS) frame. The transmitting station is allowed to transmit its packet only if the CTS frame is correctly received. The RTS and CTS carry the information of the length of the packet to be transmitted. This information can be read by any listening station, which is then able to update a network allocation vector (NAV) containing the information of the period of time in which the channel will remain busy. Therefore, when a station is hidden from either the transmitting or the receiving station, by detecting just one frame among the RTS and CTS frames, it can suitably delay further transmission and thus avoid collision.

The RTS/CTS mechanism is very effective in terms of system performance, especially when large packets are considered, as it reduces the length of the frames involved in the contention process. In fact, in the assumption of perfect channel sensing by every station, collision may occur only when two (or more) packets are transmitted within the same slot time. If both transmitting stations employ the RTS/CTS mechanism, collision occur only on the RTS frames, and it is early detected by the transmitting stations by the lack of CTS responses. The work in our research focuses on the RTS/CTS mechanisms in 802.11 DCF.

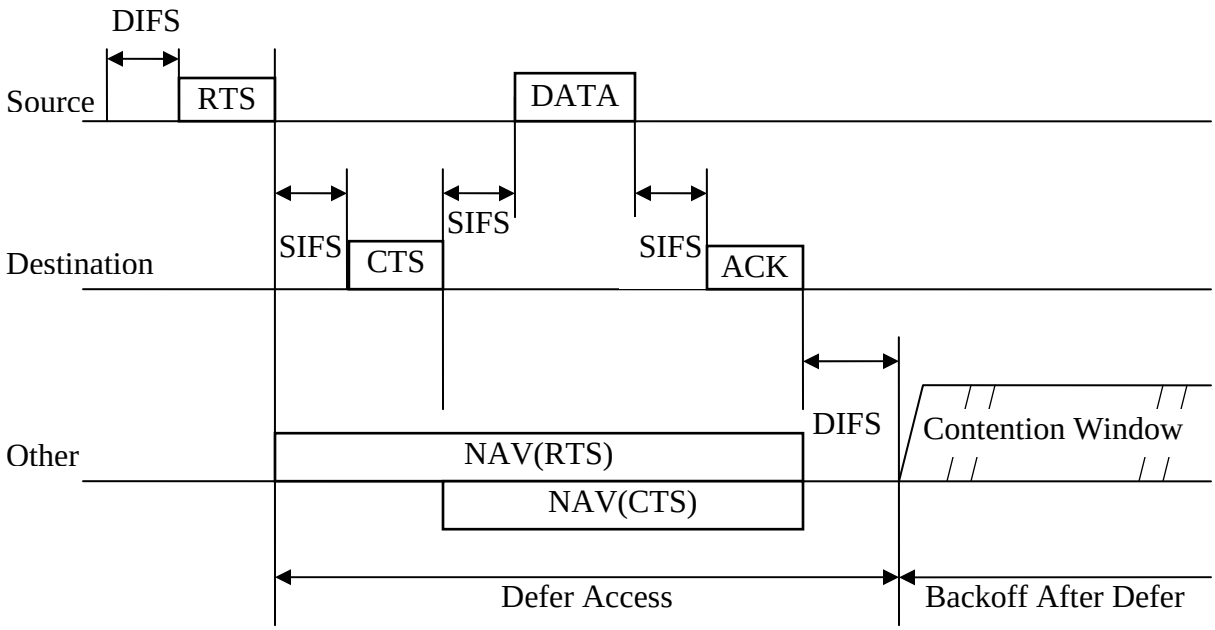


Figure 2.1: RTS/CTS four-way handshaking access mechanism.

In the literature, performance evaluation of 802.11 has been carried out either by means of simulation or through analytical models with simplified assumptions. Currently, the majority of the work on analyzing the performance of IEE 802.11 DCF has concentrated on its throughput and delay in WLANs and multihop networks. In the following subsections, we discuss the performance of 802.11 DCF in these two scenarios.

2.2.2 Performance at Single-hop Scenario

As IEEE 802.11 standard is proposed for WLANs, a large part of the existing work has focused on the throughput, capacity, and delay of the MAC protocol at single-hop scenarios in wireless networks. A *two-dimensional Markov chain analysis model* that accounts for all details of the exponential backoff has been widely used in studies analyzing and enhancing the performance of 802.11 DCF. In this model, it is assumed of constant and independent collision probability of a packet transmitted by each station, regardless of the number of retransmissions already suffered.

This model was firstly proposed by Bianchi in [11] and used to build a simple while accurate analysis model to computer the 802.11 DCF saturated throughput for both access mechanisms under ideal channel conditions in [10].

From then on, the Markov chain analysis model has been expanded to include more realistic conditions in a number of later researches. The impact of an error-prone channel over saturated throughput and delay in an IEEE 802.11 WLAN has been investigated by introducing the frame-error rates and maximum allowable number of retransmission attempts into this Markov chain model [35]. Through the model, the signal transfer function of the generalized station transition diagram is used to derive an approximate probability distribution of the MAC player service time [97]. It has also been used to analyze the performance of two types, ACK-based and leader-based, of reliable multicast at the MAC layer for IEEE 802.11 WLANs in terms of frame holding time at the AP [6], improve the performance of TCP over WLANs [91], investigate the effect of flow multiplexing over the shared channel in 802.11-based single-hop scenario [9], and compute the average service time and jitter experienced by a packet in a saturated IEEE 802.11 single-hop network [20]. This model also has been used in analyzing the emerging standard IEEE 802.11e [93, 26].

Another widely-employed model analyzing the behavior of 802.11 MAC DCF uses the *average value for a variable* wherever it is possible. This simple while effective technique provides closed-form expressions for the probability of a collision and the saturation throughput, thus facilitates the analysis of various issues, such as the choice of window size, the limit on the number of stations, and the tradeoff between collisions and backoffs. It yields two rules of thumb: halving the initial window size $CW_{\min}$ is similar in effect to doubling the number of stations, and the optimum choice of $CW_{\min}$ is proportional to the square root of packet size. This model was proposed by Tay and Chua in [79], in which the maximum throughput of the basic access mechanism in IEEE 802.11 DCF is studied. Using this technique, it showed that the 802.11

MAC can induce pacing in the traffic and a multimodal distributed traffic inter-arrival time in WLANs or ad hoc networks [80], and the delay and queue length characters in 802.11-based wireless networks are obtained in [81]. Moreover, new technique has been developed to analyze the performance of the IEEE 802.11 DCF with and without slow contention window decrease is evaluated under unsaturated conditions [76].

2.2.3 Performance at Multihop Scenario

Recently, with the progress of research in this area, a growing number of studies on proposing analytical models for evaluating 802.11 characteristics under multihop conditions have been conducted. It is shown that the relay traffic at intermediate nodes has a great impact on the performance of 802.11-based networks.

The two-dimensional Markov chain model was expanded to analyze the IEEE 802.11 protocol under unsaturated traffic conditions for multihop networks in [7]. The impact of the upper layer routing protocol was taken into account by introducing a packet acceptance factor at each relay station. The link delay characteristics, throughput, and delay of multihop infrastructure networks were analyzed in [63] through a traffic-based network model and the Markov chain model that includes multihop behavior.

As 802.11 protocols was designed for WLANs, there are still a number of improvements need to make to adapt it to the multihop network scenario. The research on 802.11 in multihop wireless networks is still one of the hotspot in the area of wireless communications. The saturation throughput of collision avoidance protocols in multihop ad hoc networks with nodes randomly placed according to a two-dimensional Poisson distribution was studied in [87]. Based on the model analysis, a number of improvements for the IEEE 802.11 MAC at the multihop scenario were proposed.

2.2.4 Performance in Ad Hoc Networks

The studies on 802.11 MAC protocols in ad hoc networks show that data transmission in ad hoc networks involves *cross-layer interactions* between MAC-layer channel access, physical layer radio characters, and network-layer data forwarding. These interactions have significant impact on the system performance. In this subsection, studies about the interactions between different layers are discussed.

To understand how physical layer techniques may affect the MAC protocol performance, the feature of interference range is studied in [46]. The impact of frame length and the mobile speed on the saturation throughput of 802.11 DCF over correlated fading channel in mobile ad hoc network was investigated [92]. The study showed that the throughput decreases with the increase of mobile velocity and there exists and optimal frame length, which is independent of the number of nodes, to maximize throughput under certain velocity. A scalable model for channel access was proposed in [19] to take into account the effect of physical-layer parameters on the MAC protocol on the likelihood that nodes can access the channel. The throughput performance of 802.11-based multihop ad hoc networks was analyzed in [1] by investigating the impact of neighbors' behavior on the behavior of a node.

The interactions of routing and 802.11 MAC layer protocols under different mobility parameters were first studied empirically in [8]. The simulation-based experiments coupled with rigorous statistical analysis showed that it is not meaningful to speak about a MAC or routing protocol in isolation. The cross-layer problem of path coupling, which involves MAC-layer interactions that impact the performance of network-layer paths that are otherwise disjoint, based upon the characteristics of IEEE 802.11 DCF was characterized and analyzed in [27]. These interactions are shown to have significant impact on energy efficiency, throughput, and delay. The model proposed in [7] takes into account of the impact of routing protocol on MAC protocols by introducing a packet acceptance factor. The interactions between IEEE 802.11e and

routing protocols in mobile ad hoc networks are also studied [18]. The interactions of the 802.11 MAC and ad hoc forwarding and their effect on capacity of ad hoc networks are investigated in [52] through simulation and analysis. The results showed that while 802.11 MAC discovers reasonably good schedules, the capacities are markedly less than optimal for very simple chain and lattice networks with very regular traffic patterns.

2.2.5 Discussion

The above listed researches show that the performance of a scheme at IP layer should be evaluated with the underlying MAC layer protocols. On the other hand, as IEEE 802.11 is the most employed MAC protocol in wireless network systems, its performance under various scenarios should be further studied. In Chapter 3, we present our work on analyzing the performance of IEEE 802.11-based multipath multihop transmission system from the perspective of the interactions between MAC and network-layer data forwarding.

2.3 Routing and Transmission in MANETs

A central challenge in the design of ad hoc networks is the development of dynamic routing protocols that can efficiently find routes between two communicating end nodes. The routing protocol must be able to keep up with the high degree of node mobility that often changes the network topology drastically and unpredictably. The routing algorithms can be divided into *single-path* routing and *multipath* routing.

2.3.1 Single-path Routing and Transmission

Single path routing and transmission is the basic routing and transmission mechanism in mobile ad hoc networks. The majority of the existing work on MANETs implements such type of

mechanism for communication between two end nodes. The routing can be divided into *proactive*, *reactive,* and *hybrid* approaches.

Proactive routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. Due to the frequent topology change in MANETs, proactive protocols suffer the disadvantage of additional control traffic needed to continually update stale routing entries. The typical examples of proactive routing protocols are Destination Sequenced Distance Vector Routing Protocol (DSDV) [68] and FSR [42].

Reactive routing, also known as on-demand routing, creates and maintains routes only when desired by the source node. Compared to proactive routing, reactive routing consumes far less bandwidth for maintaining the routing tables at each node when only a small subset of all available routes is in use at any time. However, reactive has some inherent limitations, such as long delay, increased network traffic from route maintenance, and uneasiness to support QoS. AODV [69] and DSR [13] are the two most-widely studied on-demand ad hoc routing protocols.

Work has been done to combine the advantages of proactive and reactive approaches, called hybrid routing. One reasonable middle point is to keep track of multiple routes between a source and a destination node. Another is to reduce the periodic routing overhead of proactive protocols by using some on-demand characteristics in the distance vector protocols. Examples of this type of protocols are preemptive routing proposed in [32] and Adaptive Distance Vector (ADV) routing algorithm [12].

Increasing a node's transmission range by increasing its transmission power enables direct communication with a more distant node to get reduced-hop backbone topologies. But it also increases interference since a node's transmissions will be received at higher power and by a larger number of nodes. Based on this observation, different *cluster-based routing* schemes and the associated clustering methodologies are proposed, i.e., non-adaptive clustering and adaptive

clustering, hierarchical proactive routing and hybrid routing. Typical examples of such protocols are Zone Routing Protocol (ZRP) [34] and Dynamic Group Routing (DGR) [21].

2.3.2 Multipath Routing Algorithms

Multipath routing is effective in wireless ad hoc networks since connectivity along multiple paths is less likely to be broken. As the network topology changes, failures may occur on active routes, resulting in the need for new route discoveries if only single path per flow is maintained. Frequent route discovery would, however, increase routing overhead and increase mean and peak packet latency. Using multiple paths simultaneously per flow can be a solution to these problems.

There are many algorithms proposed to search multiple paths between the end nodes. Most of them are developed from the existed and well-studied DSR and AODV single-path routing algorithms. There are also multipath routing algorithms aimed at improving a particular system performance or specified to the sensor network system. In the following, we discuss these algorithms in detail.

1. DSR-Based Multipath Routing: DSR itself can provide multiple paths from source to destination. These paths are used as backups for the primary route. The DSR-based multipath routing protocols attempt to establish more paths between the end nodes more efficiently through modifying and enhancing the original DSR protocol. A multipath extension supporting multipath video communication is proposed in [89]. The Multipath Source Routing (MSR) [88] is proposed to distribute load among multiple paths based on the measurement of RTT. It improves the packet delivery ratio and the throughput of TCP and UDP and reduces the end-to-end delay and the average queue size while adding little overhead. Two on-demand methods, the selective broadcast method and the heuristic redirection method, are proposed in [90] to effectively search for multiple node-disjoint paths between end nodes. Another routing scheme, called Split Multipath Routing (SMR) [51], establishes and utilizes multiple maximally disjoint paths. All

these protocols try to distribute data packets into multiple paths of the active sessions to make the traffic distribution efficiently utilize available network resources and prevent nodes along the data transmission path from being congested in heavily loaded traffic situations, which may happen in single-path transmission.

2. AODV-Based Multipath Routing: AODV does not have mechanism to find out multipath from the source to the destination. Some multipath routing algorithms attempt to introduce multipath searching mechanism into the AODV protocol and thus obtain multiple paths between the end nodes. A protocol, known as Ad hoc On-demend Multipath Distance Vector (AOMDV) [60], contains multipath extensions to AODV and discovers multiple paths between the source and the destination in every route discovery. Multiple paths computed in AOMDV are guaranteed to be loop-free and disjoint. Node-Disjointness-Based Multipath Routing Protocol (NDMR) [54] is a modification and extension of AODV that includes the path accumulation feature of DSR in route request/reply packets so that lower route overhead is employed to discover multiple node-disjoint routing paths. Compared to the other on-demand multipath protocols, NDMR reduces routing overhead dramatically and achieves multiple node-disjoint routing paths. AODV-Multipath (AODVM) [95] is anther modified version of AODV protocol that discovers multiple node-disjoint paths from a source to a destination.

3. Improving-Performance Multipath Routing: a routing protocol called Caching and Multipath (CHAMP) Routing Protocol [84] uses cooperative packet caching and shortest multipath routing to reduce packet loss due to frequent route breakdowns. An ant-based multipath routing protocol [44] considers both energy and latency. For latency-critical traffic, energy-pheromone and delay-pheromone metrics are combined after being normalized so that their respective significance is preserved. For not latency-critical traffic, only energy-pheromone metrics are used. The Shortest Multipath Labeled Distance Routing (SMLDR) [5] searches multiple paths between the end nodes by maintaining the ordering of distance invariants and

using the concept of limiting distance. In order to enhance the security on the existing development efforts of 802.11-based wireless networks, a multipath ad hoc routing technique, called Secure Multipath Source Routing (SMSR) [50], combats the link insecurity problem and enhances data confidentiality against eavesdropping at a higher protocol layer. This approach does not require the application to use sophisticated encryption technologies that may be too heavy burdens for mobile devices. This work is very similar with the routing algorithm proposed in [57]. A distance vector routing algorithm MDVA [86] uses a set of loop-free invariants to prevent the count-to-infinity problem in distributed Bellman-Ford (DBF) algorithm and computes multiple paths that are loop-free at every instant.

4. Multipath Algorithms for Sensor Networks: an essential requirement for adaptive routing in sensor networks is to account for the high cost associated with the use of battery power and network bandwidth. Multipath routing algorithms in sensor networks provide extensive scope for adaptively routing and dispersing traffic over such a network. Two kinds of multipath schemes, disjoint multipath and braided multipath, are constructed in [29] to enable energy efficient recovery from failure of the shortest path between the source and the destination. The braided multipath scheme results in several partially disjoint multiple paths, and it is found to be a viable alternative for energy-efficient recovery from isolated and patterned failures. A multipath routing protocol [43] primarily designed for loading balancing in sensor networks is enhanced by exploring the use of resource reservation in achieving QoS aware multipath routing. The Adaptive Multi-path Routing Algorithm (AMRA) [77] was built over AODV structure to diffuse the traffic within the network such that energy consumption is minimized.

2.3.3 Multipath Routing Analysis

In addition to the multipath routing algorithms discussed in the above subsection, the performance of multipath routing protocols for mobile ad hoc networks has also been analyzed in

the literature. The modeling frameworks provide foundations for further research on improving the system performance. In this subsection, we focus on discussing the existing work on analyzing the multipath routing mechanism in DSR and the performance of multipath routing.

1. Multipath Routing in DSR: an early analysis work [64] shows how intelligent use of multipath routing techniques can reduce the frequency of query floods in DSR protocols. In [64], an analytic modeling framework was developed to determine the relative frequency of query floods for various techniques. The model shows that while multipath routing is significantly better than single-path routing, the performance advantage is small beyond a few paths and for long path lengths. It also shows that providing all intermediate nodes in the primary path with alternative paths has a significantly better performance than providing only the source with alternate paths. A comprehensive analytic model for the performance study of the DSR protocol with multiple paths was developed in [53]. Two performance metrics, probability of a successful data transmission and probability that the multiple routes can support the next data transmission, are introduced. Both probabilities for the general case over n multiple paths are derived. These analytical results provide insights into the mechanics of the multiple DSR routing protocol. It is also useful for the design and implementation of the on-demand routing for MANETs.

2. Performance of Multipath Routing: a network model studying the scheme of load balancing in the DSR-based multipath routing MSR was established in [98]. The effect of distributing input traffic among multiple paths in MSR was analyzed. A network queuing model that incorporates the cross-traffic among these paths was established. Based on this work, an analytical modeling framework [22] was proposed to investigate multipath routing in multihop ad hoc networks. It considers the single-path model as a multi-node M/M/1 tandem network and the multi-path model as a set of multiple parallel paths. This proposed framework allows us to investigate issues such as optimal load distribution, end-to-end delay, and multipath routing reliability in ad hoc networks. The reactive single-path and multipath routing with load balance

mechanisms in ad hoc networks are compared and analyzed in terms of overhead, traffic distribution, and connection throughput in [70]. The results reveals that in comparison with general single-path routing protocol, multipath routing mechanism creates more overheads but provides better performance in congestion and capacity provided that the route length is within a certain upper bound with is derivable.

2.3.4 Multipath Transmission

Multipath Data Transmission (MDT) has been studied to provide load balance, support real-time and multimedia applications, and secure data transmission in ad hoc networks. Researches in this area involve studies of multipath description coding (MDC) [3] that was proposed for self-healing and fault-tolerance in digital communication networks. By combining multi-stream coding with multipath transport, the schemes proposed in [59] shows that, in addition to traditional error control techniques, path diversity provides an effective means to combat transmission error in ad hoc networks. The effectiveness of combining MDT and MDC for video and image transmission in a multihop mobile wireless network has been studied in [33].

The TCP performance over a multipath routing protocol was investigated in [55]. It was found that using multipath paths simultaneously may actually degrade TCP performance, partly due to frequent out-of-order packet delivery via different paths. By using the backup path routing scheme, TCP is able to gain improvements against mobility. To combine multipath routing with single-path transmission, the contention-based path selection (COPAS) [23] incorporates disjoint forwarding and reversal paths in order to minimize the conflicts of TCP data and ACK packets and solve the capture problem in mobile ad hoc networks. Hence, single-path transmission with multipath routing would be more suitable for TCP traffic in mobile ad hoc networks.

The combination of multipath routing and multiple description coding in ad hoc networks was studied in [25] through simulations from a network perspective with a realistic medium

access control protocol (IEEE 802.11) and a widely used routing protocol (DSR with multipath extensions). The simulations show that for most of the cases considered, the combination of multipath routing and MDC does not perform better than single-path routing and a single description in IEEE 802.11-based wireless networks.

An analytical framework was developed [82] and extended [83] for evaluating multipath routing in mobile ad hoc networks to combat the inherent unreliability due to nodal mobility and changes in wireless propagation conditions in these networks. Multipath transmission is used to increase the probability that essential portion of the information is received at the destination without incurring excessive delay. The probability of reconstructing the original information at the destination is derived analytically. It is shown that, under certain constraints, the packet dropping probability decreases as the number of used paths is increased. The work has been extended to general case, where the paths are not necessarily independent and their failure probabilities vary. A function that measures the probability of successful transmission is derived as a tight approximation of the evaluation function P_{succ}.

2.3.5 Discussion

The existing researches on multipath routing and transmission system demonstrate that multipath routing is an efficient mechanism to guarantee reliable communication in mobile ad hoc networks while minimizing the control overhead for route discovery and maintenance and multipath transmission provides fault-tolerant and QoS support for the system. However, for TCP traffic in MANET, multipath routing with single-path transmission is more suitable for mobile network environments.

2.4 Summary

The existing schemes securing data transmission in the mobile ad hoc networks focus mostly on improving data transmission mechanism. They have not taken into account the effect of medium access control (MAC) layer protocols and routing algorithms on the data transmission system. It has been proven that the routing protocols as well as the interactions between MAC layer protocols and data forwarding on network layer have great impact on the performance of a mobile ad hoc network. In this dissertation, we propose a strategy to enhance communication security in mobile ad hoc networks through multipath routing. It takes into consideration of the effect of underlying protocols in designing and comprehensive evaluating of a secure scheme. Our design has been driven by the following four goals:

- *Efficiency:* an ad hoc network may suffer different types of misbehavior formed individually or cooperatively. For example, some of the misbehaving nodes may form misbehavior individually while others cooperate in forming misbehavior in such a network. It would be hard for the network to run different schemes for different types of misbehavior. Therefore, a secure scheme that can tackle several types of misbehavior using the same mechanism is desirable.

- *Cross-layer:* the communication within a wireless network involves the cross-layer interactions between different layers. The benefit of underlying layer protocols should be taken while their negative effect should be minimized in secure schemes for such a network.

- *Scalability:* this scheme can be modified in various ways to provide further data protection and better system performance.

- *Moderate overhead:* an ad hoc network can be composed of a large number of nodes. The overhead generated by this scheme should be kept as low as possible.

Chapter 3

IEEE 802.11 Performance Analysis

This chapter focuses on performance evaluation of multipath transmission system over multihop IEEE 802.11-based wireless ad hoc networks. This study is conducted from a cross-layer perspective rather than only focusing on the operation and performance analysis of 802.11 MAC at one single node. The effects of both 802.11 MAC protocols and network-layer multipath data forwarding are taken into account in the system modeling. The results suggest that the interactions between 802.11 MAC and multipath forwarding affect the system performance dramatically. These models have been validated using extensive simulations under various scenarios.

This chapter consists of the following sections. The definition of the 802.11-based multipath transmission system is presented in Section 3.1. In Section 3.2 analytical models are developed to emulate the impact of 802.11-based multipath multihop transmission on frame service time at the source station for two packet generation schemes under unsaturated conditions. This time is crucial for estimating the end-to-end delay in the system. The throughput of multihop multipath transmission in 802.11-based wireless networks is investigated in Section

3.3. The simulation models implemented to validate the proposed analytical models are presented in Section 3.4, and the performance evaluation of models by means of simulation is discussed in Section 3.5.

3.1 System Definition

In this section, the multipath data transmission system is presented and the backoff scheme in IEEE 802.11 DCF that related to our modeling work is briefly described. All of the notations used in this chapter are summarized in Table 3.1.

3.1.1 Multipath Transmission System

It is assumed that the transmission rate of the wireless link is C bits/sec. The average frame arrival interval at source is $1/\lambda$. According to multiple description coding (MDC), given K paths between a pair of stations, a frame of size D_{size} is split into K packets at the source station. Thus, the packet size is D_{size}/K. In the RTS/CTS mode of 802.11 MAC protocols, the time required for one of these packets being successfully transmitted over one hop is

$$T_{suc,K} = RTS + CTS + T_d / K + ACK + 3SIFS + DIFS, \tag{3.1}$$

where T_d corresponds to the transmission time of a data packet with size D_{size}. $T_d = D_{size}/C$.

3.1.2 Backoff Scheme in 802.11 DCF

In an 802.11 MAC-based wireless network, if a station intends to initiate a packet transfer and senses the channel as busy, it defers this transmission until the end of the ongoing transmission. Then, it initializes its backoff timer, which is decreased every time the channel is sensed as idle

and suspended when the channel is sensed as busy. The station sends out the first queued packet when its backoff timer has a value of zero and the channel is sensed as idle. In the case of collision, the contending stations update their backoff timers according to the exponential backoff scheme in 802.11 DCF and begin the next transmission attempt. The channel then stays busy for duration of T_{col} before the contending stations start to decrease their backoff timers again. The time T_{col} is defined as

$$T_{col} = DIFS + RTS \,. \tag{3.2}$$

At the k-th transmission attempt, the backoff timer at a station is set to a random value $T_{BO}(k)$, which is defined as

$$T_{BO}(k) = Ramdom(k) \times SlotTime \,, \tag{3.3}$$

where *SlotTime* is the system time slot that is set by the physical layer in IEEE 802.11 standard, and *Random*(k) is a pseudo-random integer uniformly drawn from the interval [0,CW(k)]. CW(k) is the size of contention window at the k-th transmission attempt. It is an integer in the range from $CW_{\min}$ to $CW_{\max}$, which are the minimum and maximum contention window sizes respectively. The contention window size CW(k) at the k-th transmission attempt is determined as follows:

$$CW(k) = \min[CW_{\max}, 2^{k-1}(CW_{\min}+1)-1] \qquad k \geq 1 \,. \tag{3.4}$$

The maximum backoff stage in 802.11 DCF is

$$S_m = \log_2[(CW_{\max}+1)/(CW_{\min}+1)]+1 \,. \tag{3.5}$$

Table 3.1: Notations used in our modeling work.

Notation	Explanation
T_{total}	total observation time
D_{rcv}	number of data frame received
D_{size}	data frame size
$Nhop_i$	number of hops on the *i*-th path
$T_{suc,K}$	successful transmission time of a packet with size D_{size}/K over one hop
T_d	transmission time of a data frame
T_{BO}	backoff time when $CW = CWmin$
$T_{BO,i}$	packet service time increment along the *i*-th path due to 802.11 backoff scheme
$T_{BO}^{[k]}$	backoff time at the *k*-th transmission attempt
T_{col}	collision time
$T_{s,1,B}$	basic frame service time of one-hop path
$T_{s,K,B1}$	basic frame service time for round robin generation when there are *K* paths
$T_{s,K,B2}$	basic frame service time for batch generation when there are *K* paths
$T_{a,1,M}$	frame service time increment of one-hop path for Poisson arrival process
$T_{a,K,M1}$	packet service time increment for round robin generation and Poisson process when there are *K* paths
$T_{a,K,M2}$	frame service time increment for batch generation and Poisson arrival process when there are *K* paths
$T_{s,1,M}$	frame service time of one-hop path for Poisson arrival process
$T_{s,K,M1}$	frame service time for round robin generation and Poisson arrival process when there are *K* paths
$T_{s,K,M2}$	frame service time for batch generation and Poisson arrival process when there are *K* paths
S_m	the maximum backoff stage
$T_{i,m}$	one-path packet transmission time
$Diff_i$	Difference between basic 1-hop packet transmission time and packet generation interval

If a packet is transmitted successfully, the value of contention window size at a station CW reverts to $CW_{\min}$. IEEE 802.11 regulates an insertion of a backoff interval after the CW value reverts to $CW_{\min}$ following a successful transmission even if no additional transmission is currently queued. This additional backoff time is called *tailing backoff* in [76].

In this study we focus on the steady-state system performance. Thus, the long-term characteristics such as average service time are of great interest. Backoff time $T_{BO}(k)$ is represented by its statistical expected value $T_{BO}^{[k]}$, which is

$$T_{BO}^{[k]} = \frac{CW(k)}{2} \times SlotTime \ . \tag{3.6}$$

The expected value of the backoff time corresponding to the initial contention window $CW_{\min}$ is noted as T_{BO}, where $T_{BO}=T_{BO}^{[1]}$. From the above statement, the expected value of the tailing backoff is also T_{BO}.

In this study, it is assumed that no other source and background traffic is within the considered areas. This assumption allows us to better characterize the impact of both MAC and network layers on a multipath transmission system in multihop wireless networks. Issues of node mobility and multipath routing are not considered. As long as a set of nodes are within the radio range of each other, their mobility pattern will not change the selected paths. Selecting multiple paths between a pair of nodes is not within the scope of this chapter.

3.2 Frame Service at Source

The frame service time at source *under unsaturated conditions* in a multipath multihop transmission system is presented in this section. To help focus on this issue, only data

transmission *within the source range area* is considered. In order to show the impact of multipath forwarding on the system performance, the first path is assumed to be a one-hop path. Hence, there are $(K-1)$ intermediate stations for K node-disjoint paths in the considered system in this section.

3.2.1 Model Definition

The source with buffer size N ($N > 1$) is modeled as a queuing system characterized by the frame arrival process and frame service time distribution. The system is considered to be under saturated conditions if the source always has packets to send. Otherwise, it is under unsaturated conditions. The frame arrival at source is assumed to follow a Poisson process. The shared radio channel is modeled as a single "server" with three states: transmit, added time (backoffs + collisions), and idle. As the system considered here is under unsaturated conditions, the increment of frame service time at source is mainly from the backoff time. The probability of collisions among packets from the source and its intermediate neighbors is extremely small. Thus, it is neglected in the analysis in this section.

There are two schemes by which the K packets can be generated out of one frame: *round robin generation* and *batch generation*. In the first scheme, the encoder generates one packet at a time in a round robin fashion with average interval $1/(K\lambda)$. Thus, the encoder generates packets individually and independently in a sequential manner for paths 1 through K and then back to path 1. According to the properties of a Poisson process, the average frame arrival interval is still $1/\lambda$. The source queueing system in this case is an M/G/l/N model. In the other scheme, the encoder generates K packets (one per path) and puts them into the source queue at the same time.

This is a batch generation with the size K. The source queueing system is then an $M^{[K]}/G/1/N$ model.

The frame service time at source is the sum of the service time for K packets in round robin generation. In the batch generation, it is the time from the instant that the first packet in a batch starts to contend for the channel to the instant that the last packet in the same batch is acknowledged. The packet service time at source starts at the instant that the source contends for the channel to send a packet and ends at the instant that the source receives an acknowledgement for correct reception by the intended receiver or the instant that the packet is dropped after reaching a maximum retransmit limit. When the number of paths K is 1, the frame service time is also the packet service time. It is the same for both packet generation types. When $K > 1$, as one frame corresponds to K packets, the traffic at intermediate stations on different paths depends on both the source traffic and the number of paths K. The frame service time at the source then depends on the packet generation scheme.

In the following subsections, the models of basic frame service time at the source for both round robin and batch packet generation schemes are obtained at first. Then, the models of frame service time at source of Poisson frame arrival process for both generation schemes are established.

3.2.2 Basic Frame Service Time

The basic frame service time is derived when the influence from other frames is not considered. When $K = 1$, a packet with the size of a frame is transmitted over a 1-hop path in the considered system. Its basic service time is

$$T_{s,1,B} = T_{suc,1}. \tag{3.7}$$

On the other hand, when $K > 1$, the basic frame service time needs to be analyzed based on the following packet generation mechanisms.

1. *Round robin generation*: as the packets are generated individually and independently in this mechanism, the influence of other packets is not considered in the basic packet service time. To take into account the 802.11 MAC protocols, the tailing backoff time T_{BO} is introduced into the basic packet service time, which then is ($T_{suc,K} + T_{BO}$). Thus, the basic frame service time at source is

$$T_{s,K,B1} = K(T_{suc,K} + T_{BO}). \tag{3.8}$$

2. *Batch generation*: Since the K packets of one frame are generated at the same time, the influence of other packets in the same frame needs to be considered in getting the basic frame service time. As the first packet in a batch is transmitted through the first path, i.e. a 1-hop path, in the considered system here, its basic service time is $T_{suc,K}$. Since the first packet does not activate an intermediate node, it does not introduce any channel contention to the service of its following packets. Hence, the basic service time of the second packet at source is ($T_{suc,K} + T_{BO}$). T_{BO} here is a tailing backoff time after the transmission of the first packet. The second packet, as well as each of its following packets, activates one neighbor of the source. For the i-th ($i \geq 3$) packet, there are ($i - 2$) active intermediate neighbors serving packets from the same batch. These active neighbors contend for the channel with the source and introduce a further increment to the basic packet service time. The basic service time of the i-th ($i \geq 3$) packet at source then is $T_{suc,K} + T_{BO} + \frac{i-2}{i-1}(T_{suc,K} + T_{BO})$. Hence, the basic frame service time at source is

$$T_{s,K,B2} = KT_{suc.K} + (K-1)T_{BO} + \sum_{i=3}^{K} \frac{i-2}{i-1}(T_{suc,K} + T_{BO}) . \quad (3.9)$$

Based on the above models of the basic frame service time, the models of frame service time at the source (which has a Poisson frame arrival) are established analytically in the next subsection.

3.2.3 Poisson Arrival Analysis

In the Poisson arrival process, the frame arrival intervals are independent and identically exponential distributed random variables with mean 1/λ. The probability that i frames arrive during time interval T is

$$P\{n(0,T) = i\} = \frac{(\lambda T)^i}{i!} e^{-\lambda T} \qquad T > 0, \quad i \geq 1 .$$

Due to the randomness of the frame arrival, a frame/packet arriving at a busy channel will experience an increase in its service time.

When K = 1, for a 1-hop path, the basic frame service time at source station is given by Equation (3.7). The service time of a frame arriving at a busy channel is increased by a tailing backoff T_{BO}. The probability that i frames arrive during one basic frame service time is $P_1(G = i) = P\{n(0, T_{suc,1}) = i\}$. Under unsaturated conditions, the average service time for each of these i frames is $(T_{suc,1}+T_{BO})$. The probability that other l frames arrive during the service of these i frames is $P_1(H = l) = P\{n(0, i\cdot(T_{suc,1} + T_{BO})) = l\}$. Thus, $M_{i,1} = \sum_{l=1}^{\min(N-i,1)} P_1(H = l) l T_{BO}$ is the system frame service time increment due to those l frames. The total frame service time

increment in the system is $T_{a,1,M} = \sum_{i=1}^{N-1} P_1(G=i)(iT_{BO} + M_{i,1})$. Hence, the frame service time at source under unsaturated conditions when $K = 1$ is

$$T_{s,1,M} = T_{suc,1} + T_{a,1,M}. \tag{3.10}$$

When the number of paths is larger than 1 ($K > 1$), different models of frame service time need to be developed for the two the following packet generation schemes.

1. Round robin generation: the packets are generated according to Poisson distribution with average interval $1/(K\lambda)$. The probability that *i packets* generated independently during time interval T is

$$P_K\{n(0,T) = i\} = \frac{(\lambda KT)^i}{i!} e^{-\lambda KT} \qquad T > 0, \quad i \geq 1.$$

There are $(K - 1)$ intermediate stations for K paths in the considered system. The first packet (called F1) in a frame is transmitted through a 1-hop path. Hence, it does not influence the service of the following packets.

For each packet, the increment of its service time at the source is related to the position of this packet in the source queue. There are three different cases:

i) It is the first ($i = 1$) packet waiting for service: when its previous packet is not a F1 packet with probability $(K - 1)/K$, at least one intermediate station is active during the service of this packet. As the source and its active intermediate neighbor have equal right to occupy the channel, the intermediate station incurs at least $(T_{suc,1} + T_{BO})/2$ increment in the service time of this packet.

ii) It is the i-th ($1 < i < K$) packet waiting for service: when it is a F1 packet with probability $1/K$, there are at least i active intermediate stations due to the previous i served

packets, none of which is a F1 packet. They incur an increment of $i(T_{suc,1} + T_{BO})/(i + 1)$ in the service time of this packet. When it is not a F1 packet with probability $(K - 1)/K$, there are at least $(i - 1)$ active intermediate stations due to the previous i transmitted packets. An increment of $(i - 1)(T_{suc,1} + T_{BO})/i$ is incurred in the service time of this packet.

iii) It is the i-th ($i \geq K$) packet waiting for service: following the analysis of the second case for $1 < i < K$, there are $(K - 1)$ active intermediate stations currently. The service time increment is at least $(K - 1)(T_{suc,1} + T_{BO})/K$.

Hence, the minimum packet service time increment is

$$\alpha_{i,K} = \begin{cases} \dfrac{K-1}{2K}(T_{suc,K} + T_{BO}) & i = 1 \\ \dfrac{Ki^2 - K + 1}{Ki(i+1)}(T_{suc,K} + T_{BO}) & 1 < i < K \\ \dfrac{K-1}{K}(T_{suc,K} + T_{BO}) & i \geq K \end{cases}. \tag{3.11}$$

The probability that i packets enter the source queue during the basic packet service time is $P_K(G = i) = P_K\{n(0, (T_{suc,K} + T_{BO})) = i\}$. The increment of service time in the system due to these i packets is $T1_{i,K} = \sum_{j=1}^{i} \alpha_{j,K}$. The probability that other l packets arrive during the service of these i packets is $P_K(H = l) = P_K\{n(0, i\cdot(T_{suc,K}+T_{BO}) + T1_{i,K}) = l\}$. They introduce an increment to the service time of these i packets by $M_{i,K} = \sum_{l=1}^{\min(N-i,1)} P_K(H = l) \sum_{j=1}^{l} \alpha_{i+j,K}$. $T_{a,K,M1} = \sum_{i=1}^{N-1} P_K(G = i)(T1_{i,K} + M_{i,K})$ is then obtained as the total increment of packet service time in the system. Hence, based on Equation (3.8), the frame service time at source in the M/G/l/N model under unsaturated conditions for K paths is

$$T_{s,K,M1} = K(T_{suc,K} + T_{BO} + T_{a,K,M1}) . \quad (3.12)$$

2. Batch generation: As shown before, the basic service time of queued packet is ($T_{suc,K}$+T_{BO}). In the M$^{[K]}$/G/1/N model, when the arrival interval between two frames is less than the basic frame service time at source given in Equation (3.9), there are at least (K + 1) packets at the source queue. The value of packet service time increment can be obtained from the case $i \geq K$ in Equation (3.11). Then, the service time of the frame that arrives at later time is $K[T_{suc,K} + T_{BO} + \frac{K-1}{K}(T_{suc,K} + T_{BO})] = (2K-1)(T_{suc,K} + T_{BO})$. Following the analysis method shown above, the increment of frame service time due to random frame arrival is obtained as $T_{a,K,M2} = \sum_{i=1}^{N/K-1} iP_b(G=i)[(2K-1)(T_{suc,K} + T_{BO}) - T_{s,K,B2}]$, where $P_b\{G=i\} = P\{n(0,T_{s,K,B2}) = i\}$. The frame service time at source under unsaturated conditions is

$$T_{s,K,M2} = T_{s,K,B2} + T_{a,K,M2} . \quad (3.13)$$

3.2.4 Discussion

The above analytical models show that, the frame service time at source under unsaturated conditions depends on the number of paths, the size of frames, the packet generation scheme, and the backoff status in the system. The frame service time at source under unsaturated conditions for other frame arrival processes can be obtained in a similar fashion as the above analysis for Poisson arrival process. The frame service time under saturated conditions has been fully studied, but due to the page limitations, is not included here.

3.3 System Throughput

In this section, we develop an analysis model to evaluate the throughput of a multipath transmission system over 802.11-based multihop ad hoc networks. As the paths are connected only at the two end stations, the interference among different paths within 3 hops from the source and within the range of the destination needs to be considered in the throughput analysis of a multipath multihop system. The interference among the paths outside these two areas is omitted in the analysis here.

3.3.1 Within 3 Hops from the Source

It has been shown in [52] that, ideally, the RTS/CTS-based 802.11 protocols could achieve chain utilization as high as ⅓. If the transmission radios of stations that are not neighbors do not interfere with each other, only stations at least 3 hops away can send packets at the same time. It can be concluded that a new packet transmission can occur no earlier than the completion of the first 3 hops of previous transmissions [27]. Hence, the *basic* service time, i.e. the minimum necessary time, for a packet of size D_{size}/K being transmitted over a multihop path i with length $Nhop_i$ is $T_{i,m} = \min(3, Nhop_i)T_{suc,K}$.

For multiple multihop paths that are disjoint except for the source and the destination, a transmission along one path within 3 hops from the source prevents the source from sending out any packet. Accordingly, it can be concluded that a packet for one path could be transmitted from source no earlier than the first 3-hop completion of previous transmissions on all paths. As the transmissions on different paths can occur simultaneously, the maximum length of

transmission pipeline for a frame can be obtained as $\sum_{i=1}^{K} \min(3, Nhop_i)$ for K paths. Hence, the *basic* transmission time for a complete frame is $\sum_{i=1}^{K} T_{i,m} = \sum_{i=1}^{K} \min(3, Nhop_i) T_{suc,K}$.

The 802.11 MAC protocols and multipath forwarding may increase the packet service time in a multihop multipath system. The increment of packet service time along a path i within 3 hops from the source is denoted by $T_{BO,i}$. According to the relationship between the basic packet transmission time $T_{i,m}$ and the traffic load, which is represented by the average packet arrival interval $1/(K\lambda)$ at source, $T_{BO,i}$ can be analyzed in the following two cases:

1. $(T_{i,m} + T_{BO}) < 1/(K\lambda)$

When $(T_{i,m} + T_{BO}) < 1/(K\lambda)$, the packet generation rate at source is smaller than the basic packet transmission rate along one multihop path. The traffic is considered as under *extremely unsaturated* conditions. A new packet is generated at the source after the previous one has finished its first 3-hop transmission. Hence, the interference among different paths with 3 hops from the source can be neglected. The probability of a packet to be dropped due to exceeding the limit of multiple unsuccessful transmission attempts is extremely small and also neglected under these conditions. Thus, $T_{BO,i} = 0$.

2. $(T_{i,m}+T_{BO}) \geq 1/(K\lambda)$

Under these conditions, the transmission on one path would influence the transmission from the source to other paths and introduce increment $T_{BO,i}$ into the packet service time. Below we propose two methods to estimate the value of $T_{BO,i}$.

Method 1: Let $Diff_i$ be the difference between the basic packet transmission time through a multihop path i and the average packet arrival interval, i.e. $Diff_i = T_{i,m} - 1/(K\lambda)$. As $T_{i,m} \geq 1/(K\lambda)$,

$Diff_i \geq 0$. For a given $T_{i,m}$, a larger $Diff_i$ implies a smaller $1/(K\lambda)$, i.e. more packets generated within a time duration. This in turn corresponds to more contentions for the channel among neighboring stations in this area and consequently leads to more collisions. The stations would have larger backoff stages because of multiple packet retransmission attempts. Accordingly, there is a larger increment of packet service time $T_{BO,i}$. Thus, $T_{BO,i}$ can be estimated from the relationship between $Diff_i$ and the backoff time.

For a path i, let $B_s = \sum_{j=1}^{s} T_{BO}^{[j]}, \quad 1 \leq s \leq S_m$ be the accumulated backoff time. Two backoff stages s_i^{**} and s_i^{*} are obtained from the relationship between $Diff_i$ and B_s, where $s_i^{**} = \max\{s\}$ for $B_s \leq Diff_i$, and $s_i^{*} = \min\{s\}$ for $B_s > Diff_i$. It is easy to conclude that $s_i^{*} = s_i^{**} + 1$. Hence, $B_{s_i^*} = B_{s_i^{**}} + T_{BO}^{[s_i^*]}, 1 \leq s_i^{**} < s_i^{*} \leq S_m$. Set the middle of these two values of accumulated backoff time, i.e. $(B_{s_i^*} + B_{s_i^{**}})/2 = B_{s_i^{**}} + \frac{T_{BO}^{[s_i^*]}}{2}$, as a threshold. The increment of packet service time $T_{BO,i}$ can be estimated using the following equation:

$$T_{BO,i} = \begin{cases} 0 & if \quad Diff_i \leq \frac{T_{BO}}{2} \\ T_{BO}^{[S_i^{**}]} & if \quad Diff_i \leq B_{s_i^{**}} + \frac{T_{BO}^{[s_i^*]}}{2} \\ T_{BO}^{[S_i^{*}]} & if \quad Diff_i > B_{s_i^{**}} + \frac{T_{BO}^{[s_i^*]}}{2} \end{cases}. \tag{3.14}$$

The first case in Equation (3.14) corresponds to the special case when $s_i^{*} = 1$, then $B_{s_i^{**}} = 0$ and $T_{BO}^{[S_i^{**}]} = 0$. It should be mentioned that Equation (3.14) is only an estimate of the

packet transmission time increment due to the 802.11 backoff scheme and multipath forwarding. This expression does not provide an actual backoff stage experienced by a station.

Method 2: $T_{BO,i}$ is analyzed according to the operation of 802.11 backoff scheme in multipath forwarding. Based on the relationship between $1/(K\lambda)$ and $T_{i,m}$, there are four cases to be considered.

i) $|T_{i,m} - 1/(K\lambda)| \approx T_{BO}$. The packet generation rate for one path is very close to the basic packet transmission time along one multihop path. The maximum increment of packet service time along path i is a tailing backoff T_{BO} following the previous transmission and an initial backoff T_{BO} because of busy channel at two stations. In this case,

$$T_{BO,i} = 2T_{BO} . \tag{3.15}$$

ii) $(T_{suc,K}+T_{BO}) < 1/(K\lambda) < T_{i,m}$, i.e. $1/(K\lambda)$ is smaller than the basic packet transmission time over one multihop path while larger than that over one hop. In this case, the channel competition among the stations in the specified area should be considered.

When $K = 1$, the source and $[\min(3, Nhop_i) - 2]$ intermediate stations along the same path compete for the channel. Each collision leads to one T_{col} and an updated backoff duration. Thus, the maximum $T_{BO,i}$ is

$$T_{BO,i} = [\min(3, Nhop_i) - 2]T_{col} + \sum_{j=1}^{\min(3, Nhop_i)-1} T_{BO}^{[j]} \qquad Nhop_i \geq 2 . \tag{3.16}$$

When the number of paths $K = 2$, the channel competition from stations on the other path should be taken into consideration. The backoff procedure could be invoked at the source station or at the $[\min(3, Nhop_i) - 2]$ intermediate stations along each path. Hence, the maximum time increase $T_{BO,i}$ is

$$T_{BO,i} = T_{BO} + \sum_{j=1}^{K}[\min(3, Nhop_j) - 2](T_{col} + T_{BO}^{[2]})\} \qquad Nhop_j \geq 2. \tag{3.17}$$

When there are more than two paths in the system, i.e. $K > 2$, due to the competition among stations on more paths, $T_{BO,i}$ is evaluated using Equation (3.18) − as in case (iii).

iii) $(T_{suc,K} + T_{BO}) \geq 1/(K\lambda)$. The average packet arrival interval is smaller than the 1-hop basic packet transmission time, while the estimated throughput is not close to the system capacity. The source and [min(3, $Nhop_i$) − 1] intermediate stations along each path need to compete for the channel. The maximum time increment occurs when each contention leads to a collision at source:

$$T_{BO,i} = T_{add,1} = [\min(3, Nhop_i) - 1]T_{col} + \sum_{j=1}^{\min(3,Nhop_i)} T_{BO}^{[j]} \qquad Nhop_j \geq 2. \tag{3.18}$$

iv) When the estimated throughput on one path is close to the system capacity, all of the nodes that are within 3 hops from the source station compete with the source for the channel. The backoff procedure at each station should be considered in estimating $T_{BO,i}$. The valued of $T_{BO,i}$ is

$$T_{BO,i} = \sum_{j=1}^{\min(3,Nhop_i)}[\min(3, Nhop_i) - j](jT_{col} + \sum_{n=2}^{j+1} T_{BO}^{[n]}) + \min(3, Nhop_i)T_{BO} \qquad Nhop_j \geq 2. \tag{3.19}$$

3.3.2. Within the Destination Range

Two stations that connect with the destination D on different paths are hidden nodes to each other. They cannot forward packets to D simultaneously. One of them needs to defer its transmission by at least $T_{suc,K}$, i.e. one basic packet transmission time, when they both have a packet to forward. The maximum interference delay in the area of the destination for K paths is $(K - 1)T_{suc,K}$.

3.3.3 Throughput Model

Within the total observation time T_{total}, before the completion of all data transmissions, there is a duration of tail time of at least $T_{tail} = \max_{i=1}^{K}(0, Nhop_i - 3)T_{suc,K}$. The effective transmission time in the system is then $T_{total} - T_{tail}$. Obtained from the above analysis, the total time needed for transmitting a frame over the K paths is $T_{frame} = \sum_{i=1}^{K}[\min(3, Nhop_i)T_{suc,K} + T_{BO,i}] + (K-1)T_{suc,K}$. Therefore, the number of received frames within such time period is $D_{rcv} = \frac{T_{total} - T_{tail}}{T_{frame}}$. The system throughput is

$$Throughput = \frac{D_{rcv} \times D_{size}}{T_{total}} bits/\sec. \quad (3.20)$$

3.3.4 Discussion

This model shows that the throughput of a multipath transmission system in multihop wireless networks depends on the observation time, the number of paths, the length of each path, the traffic load, and the size of transmitted frames. The performance of the above proposed models is evaluated in the following sections.

3.4 Simulation Models

The GloMoSim [96] library-based simulator was used to validate the analytical models. In the simulation, each node has a power range of 376 meters. The service time and throughput are generated at steady state under different system scenarios. The buffer size at source station is set

to 100. Each simulation runs for 100 seconds. The simulation parameters are summarized in Table 3.2.

A multipath system, shown in Figure 3.1(a), has been used to evaluate the source queueing models proposed in Section III. This system consists of six stations; stations 1 to 5 are all within the range of source 0. There are one 1-hop and four 2-hop paths between source 0 and destination 1.

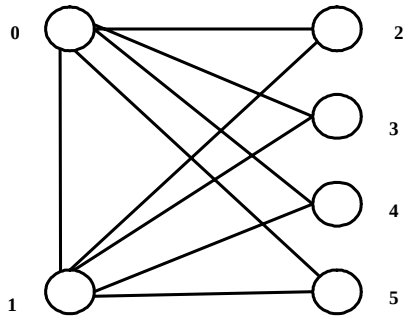
We consider the system shown in Figure 3.1(b), consisting of five multihop node-disjoint paths from source 0 to destination 1, for the evaluation multipath multihop transmission system throughput model. The length of the primary path is 3. The length of the other paths is 5. The frame arrival interval time is fixed to be 0.01 second. The frame size is changed according to the traffic load.

3.5 Validation and Analysis of Models

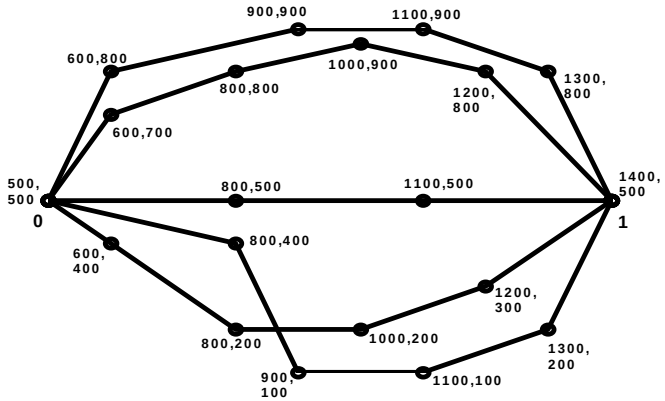
The proposed analytical models are validated by means of simulation that has been specified in the above section. The analytical results are compared with the simulation results, and the performance of the proposed models are discussed in detail here.

Table 3.2: Simulation parameters of the 802.11 MAC protocols.

Parameter	**Value**
Channel bit rate	2Mb/s
PHY preamble/header	192μs
MAC header	224μs
Packet payload size	128, 256, 512, 1024, 2048bytes
DIFS	50μs
SIFS	10μs
Slot time	20μs
RTS	282μs
CTS	258μs
ACK	298μs
Initial backoff window	31
Maximum backoff stage	5
Short retry limit	7
Long retry limit	4



(a) Source queueing model topology.



(b) Multipath multihop system throughput model topology.

Figure 3.1: Topologies for validation of models.

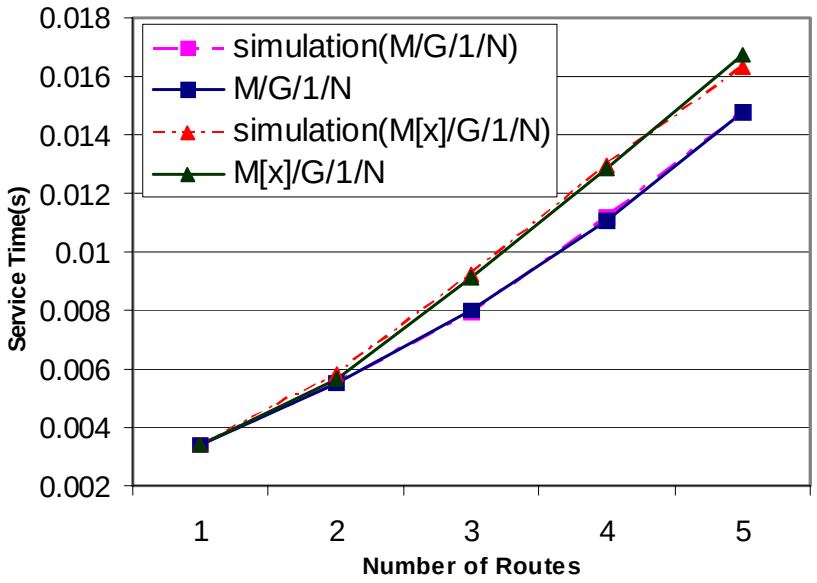


Figure 3.2: Frame service time at source station under unsaturated conditions.

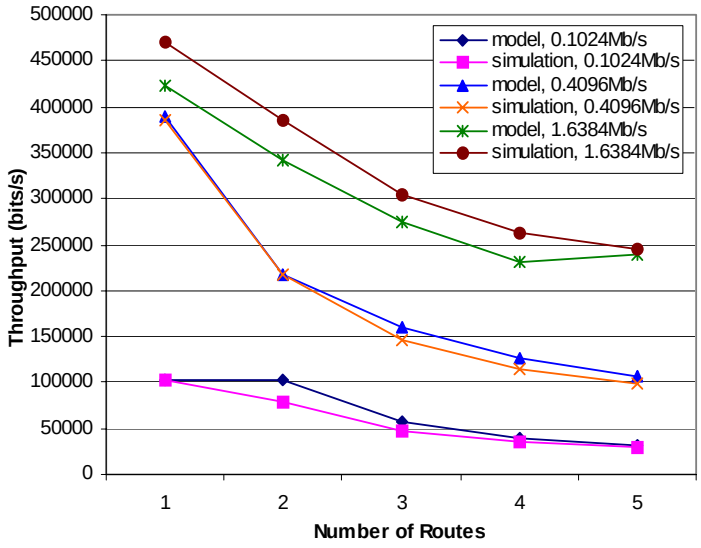
3.5.1 Source Queueing Models

Figure 3.2 shows the frame service time at source station in IEEE 802.11-based multipath multihop transmission system under unsaturated conditions. It shows a negligible difference between the proposed analytical models and simulation results for both packet generation mechanisms. This in turn indicates that the analytical models provide a very good estimate of the source queueing system. Both the analytical and simulation results show that the frame service time under unsaturated conditions increases with the number of transmission paths in the system for both models.

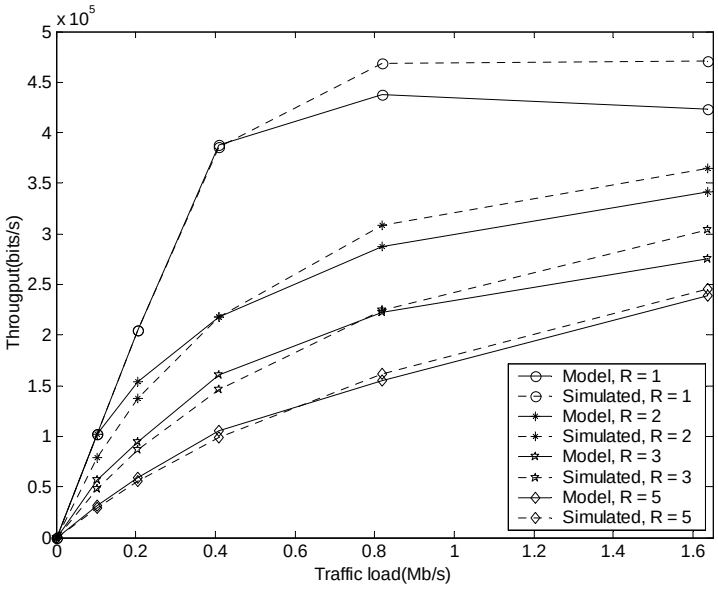
3.5.2 Throughput Model

Figure 3.3 and Figure 3.4 show analytical and simulation results of the multipath multihop transmission system throughput for different number of paths with $T_{BO,i}$ estimated using Method 1 and Method 2 discussed in Section 3.3. These comparisons show that the analytical model gives an accurate evaluation of the throughput of IEEE 802.11-based multipath multihop transmission system. Given the number of paths K, the system throughput increases with the traffic load until it attains the maximum achievable system capacity. The system throughput decreases as K increases for a given traffic load. Hence, from the perspective of the interactions between MAC protocols and network-layer data forwarding, increasing the number of paths has a negative effect on the 802.11-based multihop system throughput. Simulation results using different random seeds yielded very close results.

With $T_{BO,i}$ obtained using Method 1, the model provides a very close throughput estimate for large K or light traffic loads, as shown in Figure 3.3. However, since $Diff_i$ is considered to be positive in Method 1, the increasing collisions and longer backoff time when the packet generation rate at source does not significantly exceed the packet transmission rate in system are not included in this method. This model overestimates the throughput under these conditions. Moreover, as the system utilizes the radio channel in a more efficient way than what is considered in Method 1 for small K and heavy traffic loads, the model underestimates the system throughput in these cases.

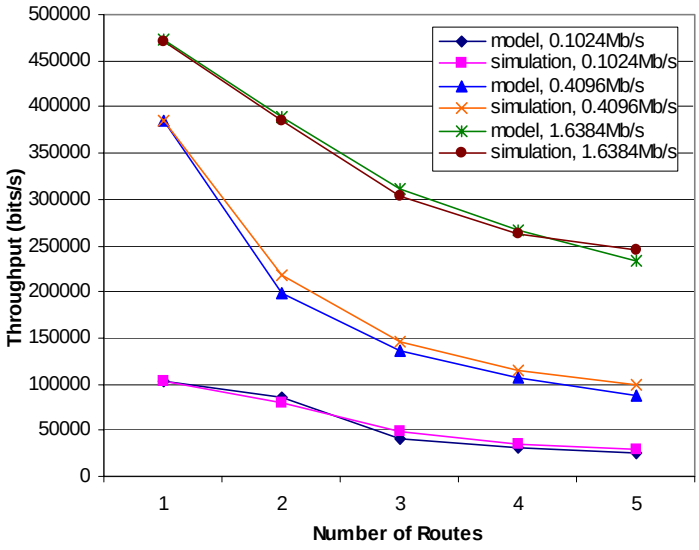


(a) Throughput versus number of routes.

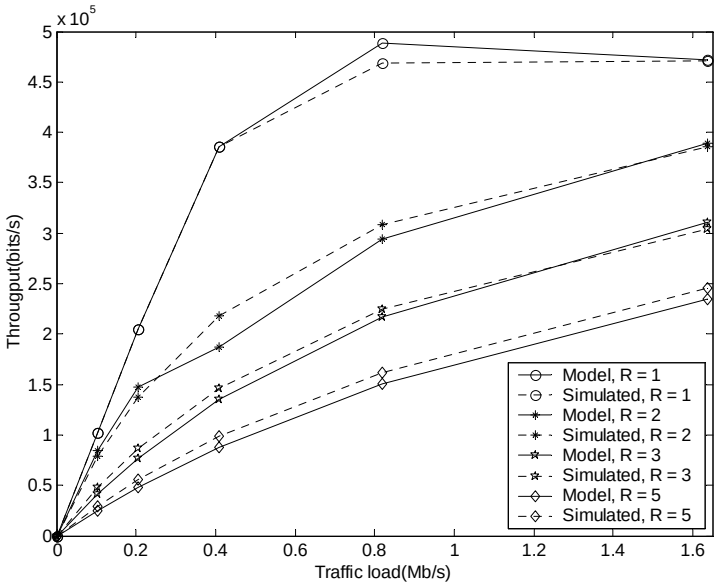


(b) Throughput versus traffic load.

Figure 3.3: Validation of system throughput obtained using Method 1.



(a) Throughput versus number of routes.



(b) Throughput versus traffic load.

Figure 3.4: Validation of system throughput obtained using Method 2.

The model provides a better system throughput estimate when $T_{BO,i}$ is obtained from Method 2, as shown in Figure 3.4. Since the IEEE 802.11 cannot discover the optimum transmission schedule on its own [52], the maximum achievable chain utilization is less than the ideal ⅓ under our simulation settings. When $K = 1$ with traffic load 0.8192Mb/s, the $T_{BO,i}$ value is obtained from one of the first three cases according to the relationship between $1/(K\lambda)$ and $T_{i,m}$. The estimated throughput is less than the ideal system capacity. But it has already exceeded the actual maximum achievable system capacity. When $K = 1$ and traffic load is 1.6384Mb/s, if the $T_{BO,i}$ valued is estimated from Equation (3.15), the corresponding throughput is close to the theoretical ⅓ chain utilization. Hence, $T_{BO,i}$ should be derived from Equation (3.19). The corresponding throughput is demonstrated to be close to the simulation result.

3.6 Summary

In this chapter, the multipath transmission system in 802.11 MAC-based multihop wireless ad hoc networks has been examined from a cross-layer perspective. Novel analytical models have been developed to provide an estimate of the MAC layer effect on network-layer multipath forwarding. The analytical models demonstrate the precise mechanism of frame service time at source under unsaturated conditions and the throughput in 802.11-based multipath multihop transmission system. A detailed description of these models has been provided.

Comparisons between models and simulation results have shown that the models provide an accurate estimate of the frame service time and the system throughput. The models show that, from the perspective of interactions between MAC and network layers, increasing the number of transmission paths has a negative effect on the performance of 802.11-based multipath multihop

transmission system. However, multipath data transmission is considered extremely useful for applications such as enhancing network security and balancing network traffic. To further enhance this study, it may be necessary to include the influence of background traffic.

Chapter 4

MARS Secure Scheme

In chapter 2, we have reviewed the existing work in the literature in the area of securing data transmission in ad hoc networks. Although a great number of studies have been done and many schemes have been proposed to address the data transmission security problem, there is still ample of room for improvements. In this chapter, we will present two novel secure schemes, MultipAth Routing Single-path transmission (MARS) and it is enhancement E-MARS, to enhance data transmission security in ad hoc networks. The MARS and E-MARS schemes are proposed from the cross-layer perspective. In these protocols, multipath routing and single-path transmission are combined with feedback mechanism to tackle misbehavior on data delivery formed by one or more misbehaving nodes in an ad hoc network.

In this chapter an analysis model of misbehavior occurrence probability in ad hoc networks is provided in Section 4.1. A brief overview of the underlying multipath routing algorithms supporting the MARS and E-MARS schemes is presented in Section 4.2. These two sections provide the necessary background for our schemes. In Section 4.3, we present an overview of our MARS secure protocol for data transmission. We further discuss the details of

the protocol and present E-MARS, an enhancement version of MARS, in Section 4.4. Section 4.5 includes the main features of the proposed schemes.

4.1 Misbehavior Analysis Models

In this section, we give out an analysis model framework that determines the occurrence of different types of misbehavior along one path in an ad hoc network. This provides a mathematical/statistical model as base for our work on securing data transmission in ad hoc networks. At first, we summarize our notations and assumptions used throughout this chapter.

4.1.1 Notations and Assumptions

This section outlines our assumptions regarding the properties of the physical and network layers. Throughput this work, we assume bi-directional communication. Such symmetry of links is needed for the transmission of the designed control packets.

We use the following notations throughout the modeling work:

- $(X * Y)$: the size of network area;
- N: the total number of nodes in the network;
- R: the transmission range of each node. We assume that the transmission of all nodes is omni-directional and the transmission range is homogeneous.
- n: the average number of hops from the source node to the destination node;
- f: the number of intermediate nodes along the path from source to destination;
- h: the average progress of each hop. This is the average distance between to nodes connected along a path.

- p: the fraction of nodes that are misbehaving in the network. This is also the probability of a node being a misbehaving node. The misbehaving nodes are selected among all network nodes randomly.
- P_{m1}: the probability of a misbehaving path, i.e. the probability of a path with at least one misbehaving intermediate node;
- P_{m2i}: the probability of two malicious nodes connected along a path due to independent route searching procedure;
- P_{m2c}: the probability of two malicious nodes connected along a path due to colluded route searching procedure;
- P_{m3c}: the probability of misbehaving path with 3 connected malicious nodes due to colluded route searching procedure.

In order to demonstrate the adverse effect of misbehavior on the network performance, we estimate the probability of misbehaving paths in this subsection. A path is defined as misbehaving when there is at least one intermediate node along the path that can be classified as misbehaving, either selfish or malicious. Our analysis is based on the following assumptions:

- The nodes are randomly distributed over the entire network area. Each node's location is independent of all other nodes' locations. There are N nodes distributed in the area of size (X * Y). In this subsection, N is set to 50 and S = X * Y = 400*400;
- The source and destination of each transaction are chosen uniform-randomly among all nodes;
- Nodes (other than source and destination) are chosen as misbehaving independently with the probability p. In this subsection, p is set to 0.03, 0.05, 0.08, and 0.10;

- The misbehaving nodes in the network are assumed to be capable of operating in two statuses: independent and cooperating;
- The Euclidean space is considered here.

We examine a path with an average number of hops n. Hence, there are $f = n-1$ intermediate nodes between the source and the destination. Each of these n paths may misbehave with probability P_m. The transmission range of each node R is set to be 120 in this section.

4.1.2 Probability of Misbehaving Path

This is the probability that there is at least one of the intermediate nodes being able to form at least one type of misbehavior along a path between any two end nodes. It is

$$P_m = 1 - (1 - p)^f . \tag{4.1}$$

The distribution of misbehaving path probability versus the length of the path is shown in Figure 4.1. Four probabilities of misbehaving node in the network are tested. From this figure we can observe that, even in the case that the probability of misbehaving nodes in the entire network area is low (8% or 10%), the probability for a path being defined as misbehaving would be still very high (more than 50%) with the increase of the length of the path, n. Hence, the number of hops along a path is very important in determining the probability of misbehaving path, P_m. In order to correctly estimate the P_m, we need to know the value of n.

The average progress of each hop, h, is essential in estimating the value of n. The value of h is derived in [56]. We cite the derive procedure here for clarity. The value of h can be approximated as the average distance between two nodes of a link. The average number of nodes in a transmission circle is

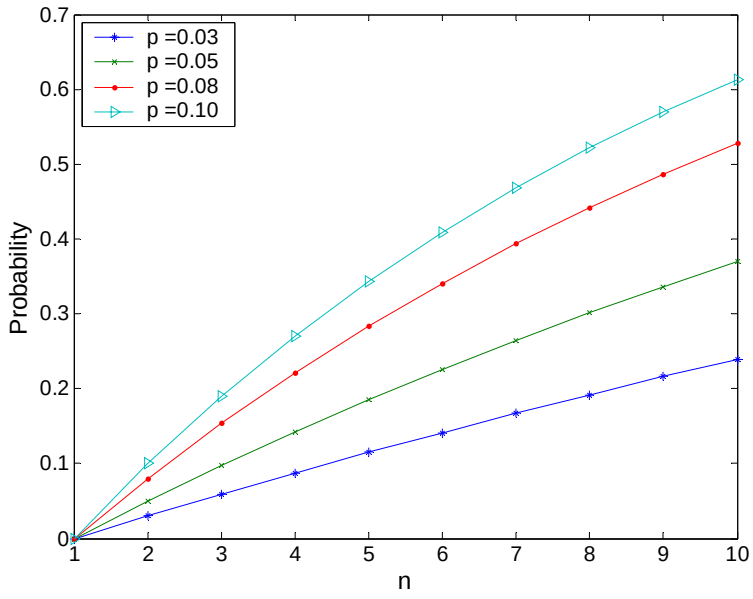


Figure 4.1: The probability of misbehaving path with n hops for different misbehaving node probabilities.

$$\alpha = \left\lfloor \frac{N}{X * Y} \bullet \pi R^2 \right\rfloor, \tag{4.2}$$

where $X * Y$ is the size of the network area and $N / (X * Y)$ is the node density. For simplicity of discussion, we assume that α is a round-down integer.

Considering the assumption of node location independence and randomness, the probability that all α nodes reside within distance r from the center of the circle is

$F(r) = P\{\text{all } \alpha \text{ nodes within a circle of radius } r\}$

$= \{P(\text{a node within } r)\}^{\alpha}$

$$= \left(\frac{\pi r^2}{\pi R^2} \right)^{\alpha}$$

$$= \left(\frac{r^2}{R^2} \right)^{\alpha} . \tag{4.3}$$

The probability density function (PDF) of r from the source is

$$f(r) = \frac{\partial}{\partial r} F(r) = \frac{2\alpha r^{2\alpha-1}}{R^{2\alpha}} . \tag{4.4}$$

The average progress of the expected value of h is then

$$h = \int_0^R r f(r) dr = \frac{2\alpha R}{2\alpha + 1} . \tag{4.5}$$

To get the average number of hops n on a path, the average distance between the source and destination in the considered network area, l, is also necessary. The value of l is the expected distance between two uniformly distributed random points in a rectangle. The probability distribution of l in a Euclidean space is shown in [30] as

$$f_L(l) = (4l / X^2 Y^2)\phi(l), \tag{4.6}$$

where $\phi(l) = \begin{cases} \pi XY / 2 - Xl - Yl + l^2 / 2 & if \quad 0 \le l \le X, \\ XY \sin^{-1}(X / l) + Y(l^2 - X^2)^{1/2} - Yl - X^2 / 2 & if \quad X \le l \le Y, \end{cases}$, assuming $X \le Y$.

The references [30] and [28] obtain different but equivalent results of the expected value of l. Here we give out the more general equation shown in [28],

$$\begin{aligned} E(l) = {} & \frac{1}{3}(X^2 + Y^2)^{1/2} + \frac{X^2}{6Y} \ln\left(\frac{Y + (X^2 + Y^2)^{1/2}}{X} \right), \\ & + \frac{Y^2}{6X} \ln\left(\frac{X + (X^2 + Y^2)^{1/2}}{Y} \right) - \frac{(X^2 + Y^2)^{5/2}}{15X^2Y^2} + \frac{X^5 + Y^5}{15X^2Y^2} \end{aligned} , \tag{4.7}$$

which, for a square of side d, reduces to

$$E(l) = \frac{d}{15} \{2 + \sqrt{2} + 5 \ln(1 + \sqrt{2})\} = 0.5214d . \tag{4.8}$$

Table 4.1: The number of hops under some widely-used settings.

Network area $X * Y$	400*400	700 * 700	1200 * 1200
Number of nodes, N	50	50	50
Transmission Range, R	120	250	376
Average number of hops, n	1.8	1.4964	1.7195

Therefore, the expected number of hops along a path can be estimated as

$$n = \frac{E(l)}{h}, \tag{4.9}$$

where we have implicitly assumed that the average progress made on a hop is independent of the average progress made on the previous hops.

The average number of hops along a path under some widely-used settings of the network area, the number of nodes, and the transmission range are shown in Table 4.1. From the table we can see that the average length of paths is about 2. The probability of misbehaving path is close to the probability of misbehaving nodes in the network.

4.1.3 Probability of Colluded Misbehaving Path

The selfish nodes form misbehavior in the system out of the intention of saving their own energy. Therefore, they would not cooperate with each other to form colluded misbehavior. Malicious nodes are controlled by enemies. They intrude into the network area with the intention to cause damage and disrupt the normal communications within the network area. They are generally equipped with more powerful facilities to cover larger transmission range and have more

calculation capacities. If they are launched by the same agent, they will be able to have the identities of each other and be aware of the malicious neighbors within their range. Due to the powerful capabilities and the intrude intentions of malicious nodes, it is a reality that they could communication with each other and form colluded misbehavior that is more dangerous and harder to be detected and mitigated. Therefore, it is very important to analyze the occurrence probability of colluded misbehavior along a path in ad hoc networks.

The probability that colluded misbehavior occurs along a path is equal to the probability that there are at least two malicious nodes connected with each other along the path. For this probability, we assume that the malicious nodes in the network conduct two different mechanisms, *independent* and *colluding*, during the route discovery and maintenance procedures.

1. Independent Routing: each of the malicious nodes is assumed to work independently during the route discovery and maintenance procedures. The probability of colluded misbehavior formed along a path is:

$$\begin{aligned} P_{m2i} &= P\{\text{at least two malicious nodes connected with each other on the path}\} \\ &= 1 - P\{\text{there is no malicious node on the path}\} \\ &\quad - P\{\text{there is only one malicious node on the path}\} \\ &\quad - P\{\text{there are more than one malicious nodes on the path, but they do not connect with each other }\}. \end{aligned} \tag{4.10}$$

The probabilities that there is no and only one malicious node along the path are:

$$P\{\text{there is no malicious node on the path}\} = (1-p)^{f}, \tag{4.11}$$

$$P\{\text{there is only one malicious node on the path}\} = fp(1-p)^{(f-1)}. \tag{4.12}$$

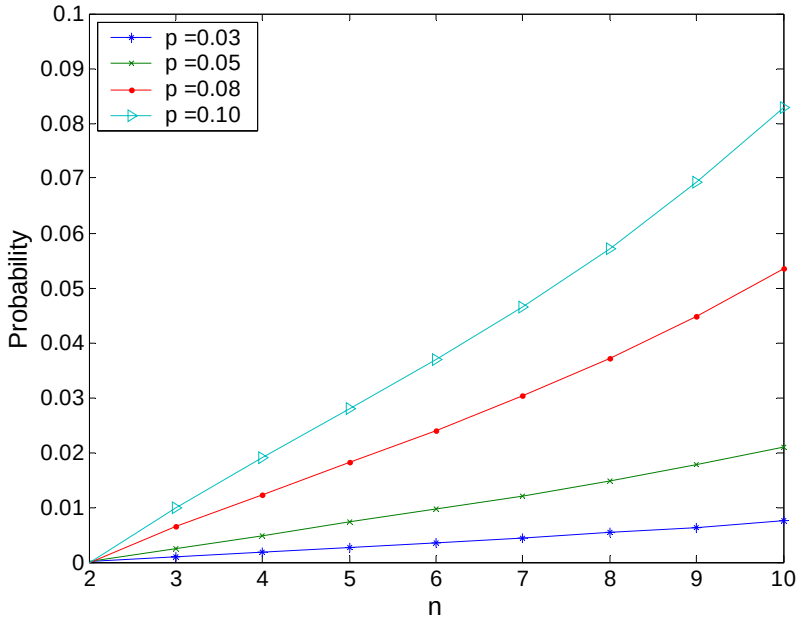


Figure 4.2: The probability of colluded misbehavior on a path of n hops for different probabilities of malicious node under independent routing.

Let $\xi = P\{$there are more than one maliciuos nodes along the path, but they do not connect with each other$\}$. In the following, we derive the value of ξ for a path with f intermediate nodes.

$$P\{\text{no 2 malicious nodes connected with each other} \mid \text{2 malicious nodes on the path}\}$$

$$= \sum_{i=1}^{f-2} ip^2(1-p)^{f-2} \qquad (f \geq 3). \tag{4.13}$$

$$P\{\text{no 2 malicious nodes connected with each other} \mid \text{3 malicious nodes on the path}\}$$

$$= \sum_{i=1}^{f-4} ip^3(1-p)^{f-3} \qquad (f \geq 5). \tag{4.14}$$

Follow this pattern, we can get that

$$\xi = \sum_{j=1}^{\left\lfloor \frac{f-1}{2} \right\rfloor} \left(p^{j+1}(1-p)^{f-(j+1)} \sum_{i=1}^{f-2*j} i \right) \qquad (f \geq 3). \tag{4.15}$$

where $\lfloor a \rfloor$ is the largest integer that is smaller than a. Combining the Equation (4.10) to Equation (4.15) together, we can get that

$$P_{m2i} = 1 - (1-p)^{f} - fp(1-p)^{(f-1)} - \xi . \tag{4.16}$$

The probability of colluded misbehaving path when the malicious nodes conduct route searching procedure independently is shown in Figure 4.2. We can see that under such situations, the value of P_{m2i} still increases quickly with the increase of the number of hops along a path.

2. Colluded Routing: if the malicious nodes in the network are capable of cooperating with each other during the routing discovery and maintenance procedures, the chances that they can connect with each other along a path will increase dramatically. By cooperating with each other during the route searching procedures, malicious nodes is capable of minimizing the formation of misbehavior-free paths while maximizing the probability of putting themselves on the selected paths for data transmission in the system. Then, they could put themselves in very powerful positions to get chance to manipulate transmitted data and launch more adverse attacks.

The cooperation during route searching procedure requires that a malicious node can be aware of all the other malicious nodes in its power range. After receiving a route request packet, instead of broadcasting the request packet to all its neighbors, the malicious node only transmits this packet to its malicious neighbor nodes. This transmission mechanism is similar with the control and data packets transmission in wormhole attack [37].

The probability that at least one of the previous $(f-1)$ intermediate nodes on a path is malicious is $1-(1-p)^{f-1}$. As all of the N nodes are distributed uniformly in an area of $(X * Y)$, the integer part of the average node number in a circle with radium R is α, which is obtained from Equation (4.2). The probability for at least one neighbor of a node be malicious then is

$1-(1-p)^{\alpha}$. Using Baye's Theorem, the probability that two cooperating malicious nodes are connected along a path between the source and the destination is:

$P_{m2c} = P$ {two or more colluding malicious nodes connected on a path}

$= P$ {at least one of the previous $f-1$ intermediate nodes on a path is malicious node & there is at least one other colluding malicious node in its transmission range}

$= P$ {there is at least one other colluding malicious node in its transmission range | at least one of the previous $f-1$ intermediate nodes on a path is malicious) P {at least one of the previous $f-1$ nodes on the path is malicious}

$$= \left(1-(1-p)^{\alpha}\right) \bullet [1-(1-p)^{f-1}] \tag{4.17}$$

The probability of colluded misbehavior on a path under such cooperating malicious condition is shown in Figure 4.3 for different values of p and the number of hops on the path. We can see that such probabilities are close to those of misbehaving path. Therefore, to provide protection to the ad hoc networks, we much take the colluded misbehavior into consideration.

Figure 4.4 shows the comparison of the probabilities of colluded misbehaving path for independent routing and colluded routing procedures. The probabilities are given out in Equation (4.16) and Equation (4.17). We can see that, in an ad hoc network, the probability for two malicious nodes connected on a path under independent route searching procedure is non-ignorable, while the probability for two malicious nodes connected on a path under colluded route searching procedure is even much higher and must be considered seriously. Based on these analysis models, the attacks formed by two connected colluding malicious nodes must be studied in-depth.

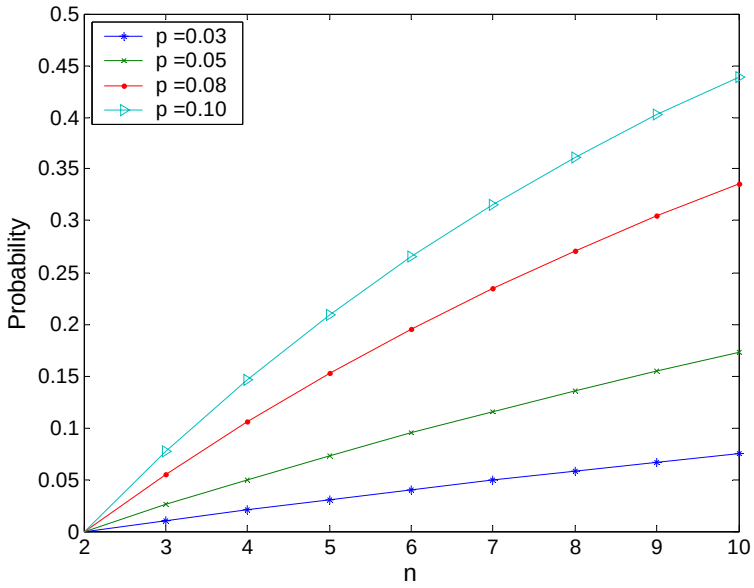


Figure 4.3: The probability of colluded misbehavior on a path of n hops for different probabilities of malicious node under colluded routing.

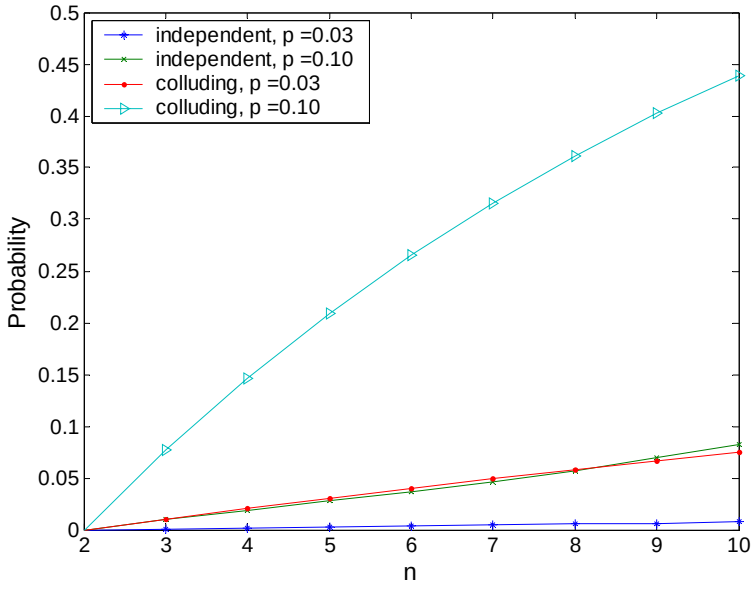


Figure 4.4: The comparison of the probabilities of colluded misbehavior for different routing mechanisms.

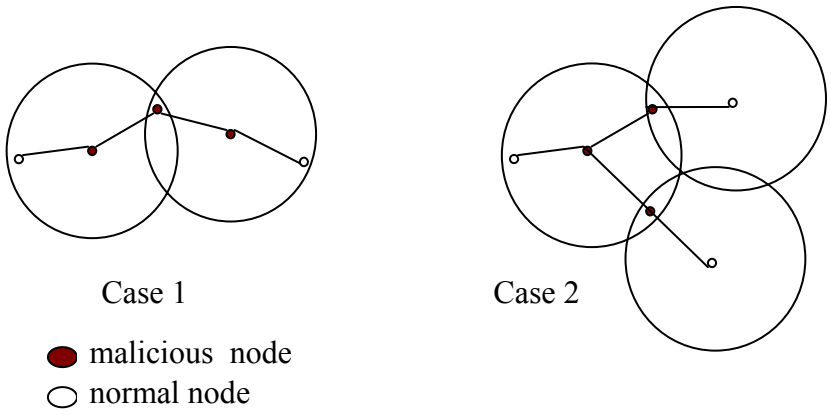


Figure 4.5: Two cases of three malicious nodes connected along two consecutive links.

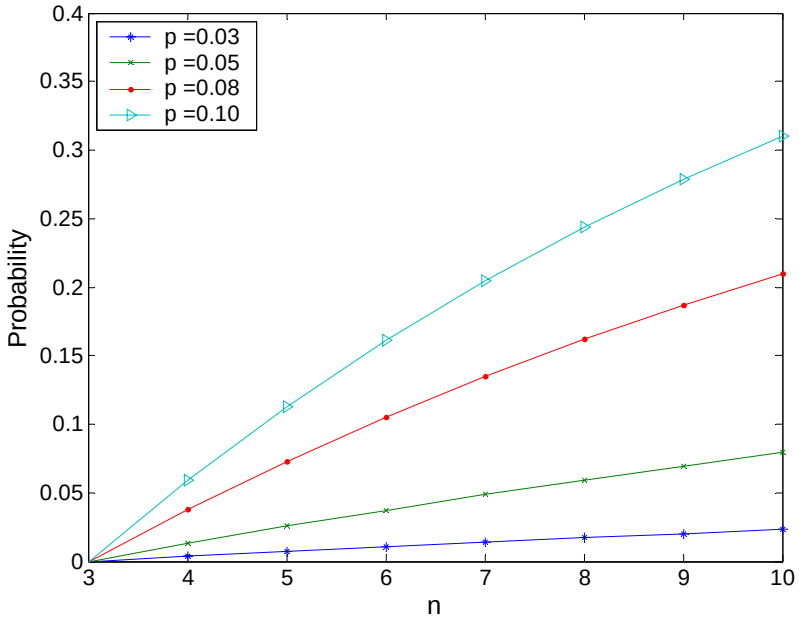


Figure 4.6: The probability that there are three or more malicious nodes connected along a path for different probabilities of malicious node.

3. More-colluded-node Misbehavior: we now further consider those cases in which more than two colluding malicious nodes are connected along a path. There are two cases, as shown in Figure 4.5, that three colluding malicious nodes are connected along two consecutive links. Case 1 illustrates that there are three malicious nodes connected along a path between two end nodes. Case 2 illustrates that two malicious nodes follow one malicious node along two different paths separately. Therefore, only Case 1 is the situation that should be considered here. Only the colluded route searching procedure is considered in the following analysis since, based on the value of P_{m2i} shown in Figure 4.2, the probability of this case under independent routing would be very small and ignorable.

Following the same method that derives out Equation (4.17), we can get the probability of three or more malicious nodes connected on a selected path. The only difference with the derivation of Equation (4.17) is that, because there needs to be a third connected malicious node on the path, the probability that there are at least one malicious node in the transmission range of the specified node need to be considered twice.

$P_{m3c} = P$ {three or more colluding malicious nodes connected on a path}

$= P$ {at least one of the first $(f-2)$ intermediate nodes is malicious & a second malicious node in its power range & a third malicious node in transmission range of the second malicious node}

$= P$ {at least one malicious node in the power range of one malicious node & at least one malicious node in transmission range of the second connected malicious node | at least one of the first $(f-2)$ intermediate nodes on the path is malicious)

$\cdot P$ {at least one of the first $(f-2)$ intermediate nodes is malicious}

$$= \left(1-(1-p)^{\alpha}\right)^2 \bullet [1-(1-p)^{f-2}] \tag{4.18}$$

Figure 4.6 shows the probability of three or more connected malicious nodes on a transmission path versus the number of hops for different probabilities that a node is malicious. Due to the limitation of wireless propagation and wireless ad hoc network capacity, the general number of hops considered is 6. It illustrates that the chances for more than two colluding malicious nodes connected on an *n* hop route also need serious considerations. The cases in which three or more malicious nodes are connected along a selected path are not considered in our work. This model we proposed here can be used in further studies of wireless ad hoc network routing procedures and schemes to secure data transmission in such networks.

4.2 Multipath Routing Algorithm

The schemes we propose in this work can operate with any underlying routing protocols that can obtain two node-disjoint paths between the source and the destination. A more efficient multipath routing algorithm can help the proposed schemes achieve larger benefits. In this section, we give a brief description of the two multipath routing algorithms employed in our research. The security of these algorithms is also discussed.

4.2.1 Routing Algorithms

Two algorithms are employed in this work to obtain multiple node-disjoint paths for the proposed schemes. One is a modified version of the optimized Dynamic Source Routing (DSR) protocol [13]. DSR is a routing algorithm that aims at obtaining single path routing. The multiple paths between a pair of nodes established from the routing procedure are generally used as

backup paths for data transmission. In the modified DSR, a source implementing DSR is capable of getting multiple paths from its route cache more efficiently.

In DSR, when a node has data for a destination and there is no path to the destination exists in its route cache, it sends out a route request (RREQ) packet. All nodes receiving this RREQ packet put themselves into the route path and forward it to their neighbors if they have not received it before. If a receiving node is the destination or has a route to the destination, it sends a route reply (RREP) packet containing the full route to the destination back to the source instead of forwarding the request packet. The source records some different routes it receives and sends data packets along the best one. In the case of a link failure, the node cannot forward the data packet to the next node sends a route error (RERR) packet to the source. Then the source uses another route in its cache to the destination to send data or sends a new RREQ packet for new paths if there is no other path to the destination in its cache.

To get more node-disjoint paths efficiently and reduce the routing overhead in the system, we made two following modifications on the single-path DSR in our implementation.

-- First, the later received RREQ packets at nodes that are not the destination will be cached in the RREQ cache of the nodes rather than being discarded.

-- Second, only the destination of the RREQ can send a RREP packet back to the source. No intermediate node that has a path to the destination can reply the RREQ packet in the system.

The other routing algorithm we implemented is the DSR-based on-demand multipath routing algorithm proposed in [90]. The broadcasting and route-searching procedures in this routing algorithm are similar with those in DSR with four main modifications.

1) The later-received RREQ in the intermediate nodes are cached instead of dropped.

2) Only the destination sends RREP packets back to the source.

3) The RREP includes a label *isRedirection* to indicate whether the RREP packet should be redirected when traversing back to the source. If the path included in the received RREQ packet is node-disjoint with all paths included in its cached RREQ, the destination sends a RREP packet to the source using the reverse path with *isRedirection* be FALSE. Otherwise, the isRedirection in the RREP sent back to the source is set to be TRUE.

4) When an intermediate node receives a RREP with *isRedirection* be FALSE, it forwards the RREP to the next node. Or else, it checks if there is a path node-disjoint with the remaining hops included in the RREP packet in its cached RREQ. If so, it redirects the RREP following this cached path and set the *isRedirection* in the RREP to FALSE.

4.2.2 Routing Security

The proposed schemes in our work are to help ensure secure data forwarding after the multiple paths between the source and destination have been established. The security of routing discovery is provided by the security mechanism integrated in the routing protocols. We use secure on-demand multipath routing algorithms in this study to provide protection for routing procedure and guarantee the correctness of established paths.

It is assumed that a security association ($SA_{s,d}$) between the source and the destination exists in the proposed schemes. It could be a symmetric shared key between them. Since two nodes choose to employ a secure communication scheme, their ability to authenticate each other is indispensable. The above two introduced multipath routing algorithms are integrated with some security mechanisms. A random query identifier (RQI) is introduced into a RREQ packet,

which carries a message authentication code (MAC) calculated from the RQI and the $SA_{s,d}$. Hence, only the destination that has a security association with the source sending out the RREQ packet can reply the request packet. A fraud RREQ packet or a fraud route reply (RREP) packet can be detected by such a mechanism.

Due to the introduction of the security mechanism into the routing algorithms, the DSR-based on-demand multipath routing algorithm implemented in our work would have some differences with the heuristic redirection method proposed in [90]. The major differences are:

--First, only an intermediate node having a security association with the source can redirect a RREP packet generated by the destination.

--Second, two node-disjoint paths with the minimum sum of hop numbers are selected

Since we focus on securing the data transmission procedure, the secure multipath routing algorithm is not discussed in more detail in this dissertation.

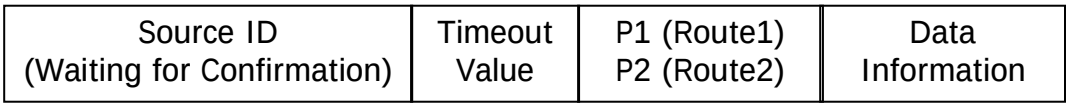
4.3 Overview of MARS Scheme

The principle of the proposed scheme is to guarantee the reception of data packets at the destination. The proposed security solution is provided at IP layer. The source selects two node-disjoint paths: one is used for data transmission; the other is used for control information exchange. This is where its name, **M**ultip**A**th **R**outing **S**ingle-path transmission (MARS), comes from. The destination detects misbehavior on data and notifies the source through a feedback mechanism. The adverse effects are mitigated without restrictive assumptions on the network nodes' trust and network membership, without the use of intrusion detection schemes, and at the expense of moderate overhead only.

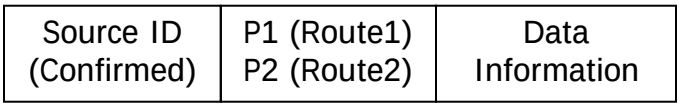
In the MARS scheme, the source keeps a Temp Route Pair List (TRPL) that contains pairs of node-disjoint paths obtained from route searching procedure. The source saves all the paths to the destination obtained from route discovery procedure in its route cache. When it receives a new path to the destination contained in a RREP packet, it compares this path with all the cached paths. If there are paths node-disjointed with the new one, the new path and each of its node-disjoint paths are put as a corresponding pair into the TRPL at the source. With the TRPL, the source can obtain valid two-node disjoint paths, R1 and R2, efficiently when it starts data transmission in the system.

The MARS scheme tackles various types of misbehavior through the use of two new types of control packets, termed INF and NTF. An INF packet, used to detect misbehavior, is sent from the source to the destination at the start of data transmission. A NTF packet, used to mitigate the adverse effects, is sent from the destination to the source when suspected misbehavior along data transmission path is detected.

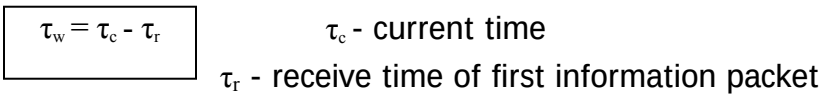
The shorter one of the selected two node-disjoint paths, R1, is used for data transmission. The longer path, R2, is used for control information exchange between the source and the destination. To help the destination monitor the performance of R1, at the beginning of one data transmission task, an INF packet is sent to the path R2 right after the first data packet queued in the source buffer has been sent out to the path R1. Both the first data packet and the INF packet contain the information about this transmission task, including the information about both paths and data generation at the source. The transmission detail of the INF packet with the corresponding data packet will be presented in the following section.



(a) waiting list.



(b) confirmed list.



(c) timer.

Figure 4.7: Lists and timer kept in destination for misbehavior detection.

To detect misbehavior on data, two lists called waiting list (WL) and confirmed list (CL), as shown in Figure 4.7, are maintained at the destination. Upon receiving a packet containing new transmission information from a source, the destination puts the source ID, a timeout value τ, and the transmission information into the waiting list. τ is the timeout value set by the destination for misbehavior detection. If the destination receives a second packet that contains matched transmission information from the desired path before the timeout expires, it admits that both paths work well currently. The source ID with the corresponding information is then moved into the confirmed list.

The destination keeps two values, *S* and *T*, to monitor the reception of data from the source after the source and the saved path information has been moved into the confirmed list. *S* is a statistic value to record the number of received data packet during an observation period *T*.

At the end of each observation time T, the destination compares the statistic reception value $Rv = S/T$ with the data generation rate value Rg that is transmitted from source and currently saved in the confirmed list.

If the destination cannot receive matched transmission information from the source within the timeout limit given by τ, it claims that the data dropping misbehavior happens along the path R1. If the value of Rv is smaller than that data generating rate to a certain extend, it claims that the partial data dropping misbehavior happens along the path R1. Under these conditions, the destination sends a NTF packet back to the source through the path R2 and removes the source ID and the corresponding items from the two lists. The misbehavior detection will be discussed in detail later in the next section.

Upon receiving a NTF packet, the source removes the indicated pair of paths from its TRPL list and route cache. If it still has data to send, the source checks the TRPL for another pair of node-disjoint paths and sends an INF and data packet containing new transmission information into them. The source initiates a route request procedure if no node-disjoint paths are available in the TRPL list. The destination would remove the corresponding items from the waiting list or the confirmed list when it receives a new RREQ from the source, and then update the lists when it receives new transmission information.

4.4 Details of MARS

In this section, the implement details of the MARS scheme are discussed. The TRPL list at source, the two new introduced control packets, the authentication of different packets, the

timeout parameter τ setting at the destination, the update of two lists at the destination are presented. The detection of various types of misbehavior at destination in the MARS is discussed.

4.4.1 The Temp Route Pair List

The Temp Route Pair List (TRPL) is kept at the source to provide the two node-disjoint paths needed in the transmission procedure. It contains the pairs of valid node-disjoint paths. The list is built during the route searching procedures. When the source receives a route error packet or NTF packet from the destination, it checks the paths in TRPL. If one path in the list is determined to be "misbehaving path" or "broken path", the indicated path and all its corresponding node-disjoint paths are deleted from the list. Figure 4.8 and Figure 4.9 indicate the building and delete procedures of this list.

4.4.2 New Control Packets

The two new control packets, INF and NTF, are introduced into the network system to exchange the transmission information between the source and the destination. An INF packet contains information of the corresponding transmission task: (a) the information of data generation at the source, such as the data generation rate R_g, the data packet size, and expected data amount during a time period; (b) the information of the data transmission path R1, including the path length and the nodes along the path R1. An INF packet can also carry a randomly generated key to authenticate the data packets of the corresponding transmission batch.

A NTF packet contains an alert identifier and the information of this pair of paths, including the lengths of paths R1 and R2 and the nodes along these two paths.

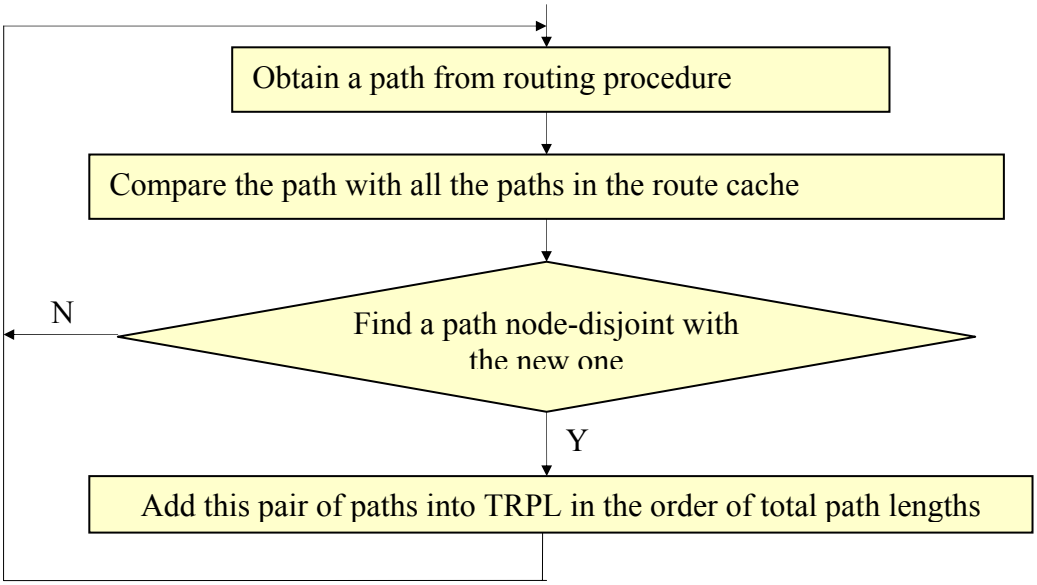


Figure 4.8: The building procedure of TRPL list.

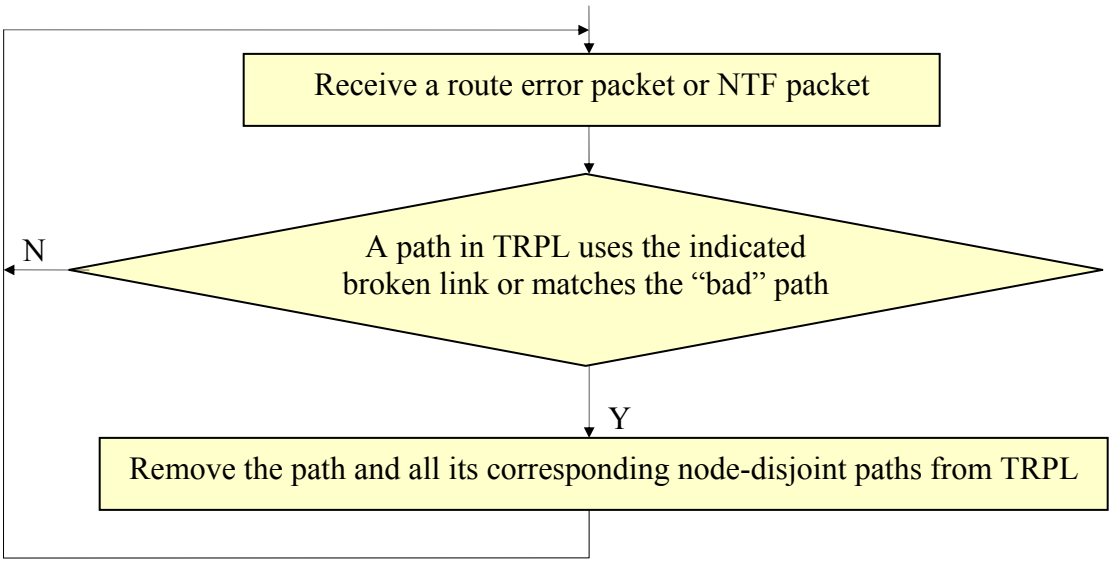
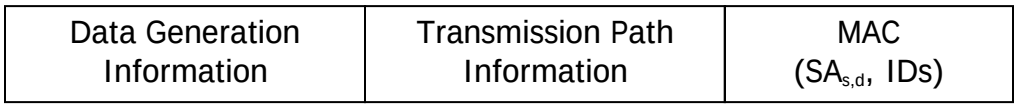
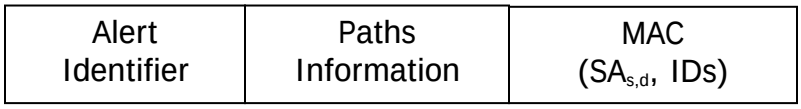


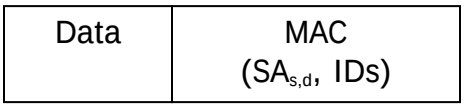
Figure 4.9: The delete procedure of TRPL list.



(a) INFO packet.



(b) NTF packet.



(c) data packet.

Figure 4.10: Structures of different packets for security transmission.

4.4.3 Transmission of Task Information

The information of transmission tasks is transmitted form the source to the destination. It is contained into two types of packets: the first data packet of a transmission task and an INF packet. An INF is sent into the path R2 after the first data packet of a task is sent into the path R1. The transmission of these two packets differs according to the following two statuses of the source buffer when the source is ready to transmit data into two valid node-disjoint paths obtained from its TRPL.

1. Non-empty Source Buffer: when the source has data to transmit without two valid node-disjoint paths to the destination, it would put the data packet into its buffer and launch the route discovery procedure. All new data packets generated during the route discovery procedure would queue at the source buffer. Then, when the source is ready to send out data, the source

buffer is not empty. One the other hand, when the source is sending out data packet queued in its buffer, and one of the two currently used paths becomes invalid due to link-broken or misbehavior notification, the source with a non-empty buffer needs to get two new node-disjoint paths and transfer the transmission into these paths.

Under the above two conditions, there would be data packets queued in the source buffer when the source obtains two valid node-disjoint paths. At the start of transmission, the source adds an information header at the first data packet in the queue. The information header contains: (a) the information of data generation at the source, such as the data generation rate *Rg*, the data packet size, and expected data amount during a time period; (b) the information of the exchange path R2, including the length of R2 and the nodes along the path R2. All the other following data packets transmitted through the same R1 do not need to be added such a header. Following the transmission of the first data packet, an INF is sent from the source into the path R2.

2. Empty Source Buffer: when the source generates a new data packet with an empty data buffer and gets two valid node-disjoint paths to destination immediately, it adds an information header, which is the same as that discussed above, at this data packet before sending it into the path R1. An INF packet is sent into the path R2 after the transmission of this headed data packet.

4.4.4 Packet Authentication

It has been mentioned in Section 4.3 that a security association ($SA_{s,d}$), such as a symmetric shared key, is assumed between the source and the destination in the MARS scheme. Since two nodes choose to employ a secure communication scheme, their ability to authenticate each other is indispensable.

Each of the data and control packets in the system carries a message authentication code (MAC) calculated from the source ID, the destination ID, and the $SA_{s,d}$. As a result, the end nodes can verify the integrity and the authenticity of these packets, whose structures are shown in Figure 4.10. The intermediate nodes are not required to authenticate the data and control packets in the system. This mechanism avoids the complexity verification operations at intermediate nodes that are employed by some other studies [56].

4.4.5 Timeout Parameter at Destination, τ

The timeout parameter τ is used to set up a time limit that the items can stay in the waiting list (WL) at the destination. If the timer expires before the matched information is received, the destination claims detecting misbehavior on data, and a NTF packet is sent back to the source. It is clear that false alarms may be triggered if τ is too small. On the other hand, if τ is too large, the destination will be too slow in detecting misbehavior, and this may cause a relatively big delay in the network. Thus, an appropriate value of τ is important for the performance of the MARS scheme.

The timeout value τ is related to the lengths of the selected node-disjoint paths and the current network traffic. It should satisfy

$$\tau > \max\left(\frac{T_1}{l}, \frac{T_2}{l'}\right)\left|l - l'\right| \tag{4.19}$$

where l and l' are the lengths of the paths, and T_1 and T_2 are the times that take a packet to transmit through a path with length l and l' respectively.

4.4.6 Lists at Destination

When a packet containing transmission information arrives at the destination, the destination checks the received information to determine if the waiting and confirmed lists should be built or updated. If the packet comes from a source to which there is no corresponding item in the two lists, the destination adds items of this source into the waiting list. If another packet coming from the same source contains the matched information are received from the expected path, the information is confirmed and the corresponding items of this source are removed from the waiting list into the confirmed list.

If new transmission information from a source is received while the previously received information of the same source is at the waiting list, the destination updates the corresponding items of this source at the waiting list with the new received information. If new transmission information is received after the previously received information of the same source is at the confirmed list, the destination removes the corresponding items of the source from the confirmed list and adds new items of the source into the waiting list for further confirmation. If the destination receives new route request packet from a source which has corresponding items in one of the lists, it removes the existing items from the lists. The complete update of the lists at the destination is presented in Figure 4.11.

4.4.7 Misbehavior Detection at Destination

In our work, the misbehaving nodes are assumed to manipulate the transmitted data but forward the control packets. The MARS can efficiently detect various types of misbehavior on data. Here, we discuss the mechanism in MARS to detect data dropping and data modification.

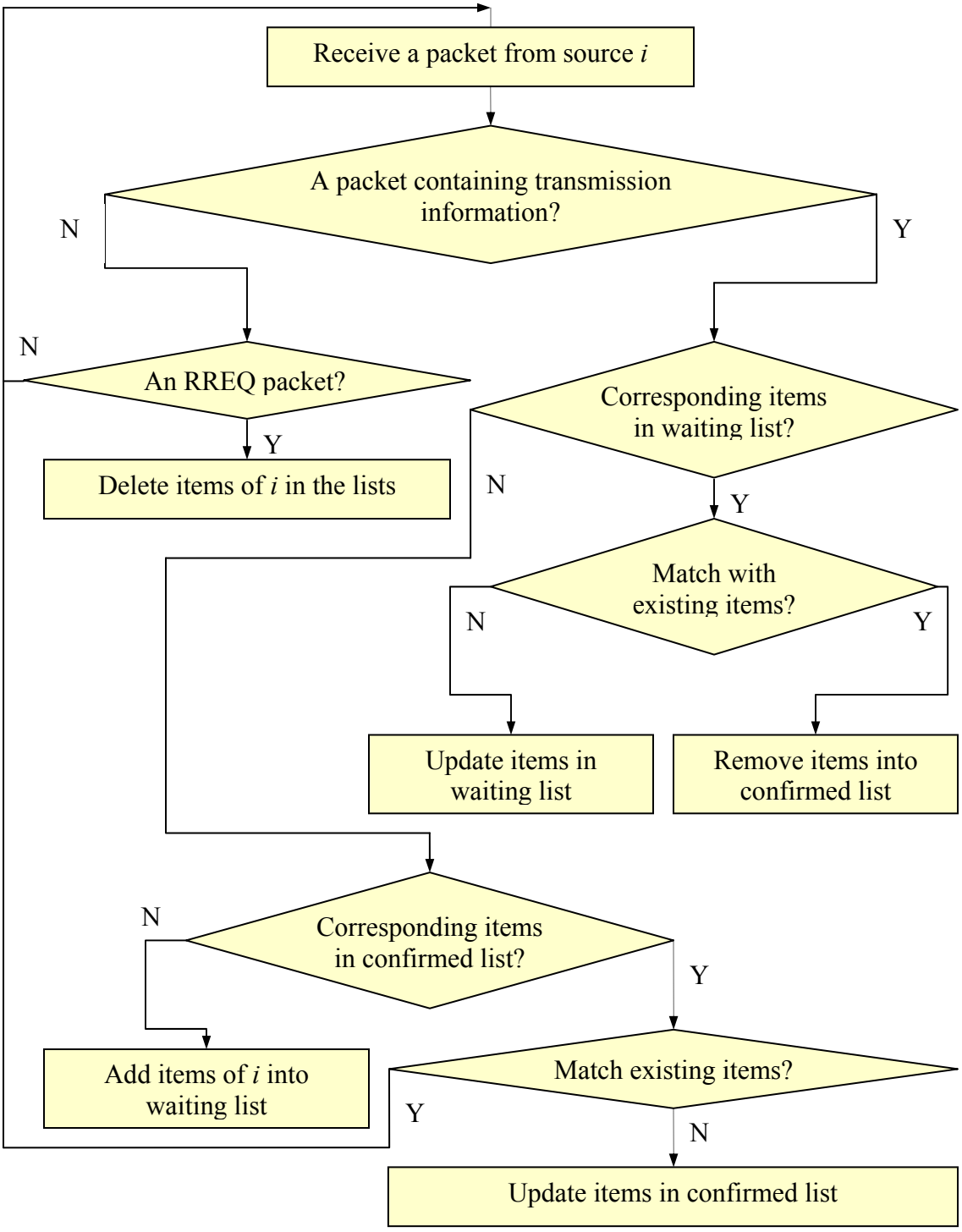


Figure 4.11: The update of lists at the destination.

If *all data packets are dropped* by misbehaving nodes along the path R1 individually or collaboratively, the destination would not receive the data packet containing matched transmission information within the timeout limit after have received the information from INF packet. The misbehavior is then detected.

If the data packets are *partly discarded* to a certain extent, the difference between the statistic value $Rv = S/T$ calculated after a period T and the data generation rate value Rg transmitted from the source and saved in the list would exceed a specified limitation. Hence, although the source and transmission information may have been moved into the confirmed list, such misbehavior would still be detected.

If the data packets are *modified* during the transmission procedure, the destination would detect the modification through calculating the message authentication code (MAC) attached in the received data packets or authenticating the data using the key delivered by INF packet.

Whenever the misbehavior is detected, the source ID and the corresponding items containing transmission information are removed from the lists. A NTF packet is then sent back to the source through the path R2.

4.5 Enhanced-MARS (E-MARS)

The delay of a data packet in the network is composed of transmission time along the path and waiting time at the source and intermediate nodes. In the MARS protocol, the time that data packets stay in the source buffer before the establishment of node-disjoint paths contributes partly to the end-to-end delay in the network. In this dissertation, we also proposed an

enhancement to the MARS scheme, E-MARS, to decrease this buffering time and improve the overall performance of the network system.

In the E-MARS scheme, the source transmits the buffered data packets through the first established path. A new generated data packet is transmitted through the shortest cached path when the node-disjoint paths are not available. No transmission information is piggybacked in these data packets and no INF packet is transmitted in the above two cases. The data transmission follows the MARS once two node-disjoint paths are available. Hence, we only point out the difference between MARS and E-MARS here instead of repeating the details of data transmission in E-MARS.

The E-MARS could decrease the end-to-end delay in the network. The cost is that the source may not be aware of misbehavior on transmitted data in time in some cases. But due to the reliability mechanism inherent in the E-MARS, the system performance is still guaranteed.

4.6 Features of the Schemes

The proposed MARS and E-MARS protocols require a security association only between two end nodes, the source and the destination. None of the end nodes needs to be securely associated with any of the remaining nodes in the network. Thus, unlike the schemes in [56, 61], the proposed MARS and E-MARS schemes do not require cryptographic operations and authentications at intermediate nodes. As there is a reliable end-to-end feedback channel between two end nodes, any misbehavior detected by the destination can be reported back to the source promptly. The schemes can detect and mitigate various types of misbehavior on transmitted data formed by individual or cooperating nodes.

The overhearing [61, 73] and some acknowledgement schemes [56, 4] can efficiently detect and mitigate misbehavior on data formed by individual misbehaving nodes. Once the misbehaving nodes in the network can cooperate with each other and form more sophisticated misbehavior, these schemes would fail to provide sufficient protection to the system. Assume that two intermediate nodes N1 and N2 are connected on a data transmission path. N1 forwards its received data packets to N2, and N2 drops them. N1 tries to cover the data dropping at N2 by ignoring it or generating fake acknowledgements. The overhearing and TWOACK schemes in [56, 61, 73, 4] cannot detect such type of colluded misbehavior. In the overhearing schemes, N1 would not report the misbehavior of N2 to the system. If the N1 node generates a fake TWOACK packet for N2, or N2 sends a fake TWOACK packet to N1, neither could the TWOACK and S-TWOACK protocols detect such fabricated packets and such type of colluded dropping. The MARS and E-MARS schemes proposed in our work can solve the problem of colluded misbehavior on data along the data transmission path.

Other misbehavior detection schemes [71, 94] put the misbehavior detection mechanism at the source node. The source needs to monitor the status of each data transmission paths, whether it implements single-path transmission or multipath transmission. Each transmitted data packet needs to be acknowledged in such mechanisms. These schemes can promptly detect suspected misbehavior on data transmission. However, the control overheads associated with them are significant. The MARS and E-MARS schemes in our work put the misbehavior detection at the destination end. By this way, the NTF packet notifying suspected misbehavior is sent back to the source only when the destination detects abnormal signal on transmission. The control overheads are therefore much fewer and the performance of the system is guaranteed.

Chapter 5

Performance Study

This chapter presents a comprehensive performance study of the proposed MARS and E-MARS protocols. Firstly, we present in Section 5.1 the simulation results to show the correctness and effectiveness of the MARS and E-MARS schemes in protecting data transmission under different types of misbehavior in wireless ad hoc networks. Secondly, a more detailed simulation study is presented in Section 5.2. We study the performance of these two protocols in different scenarios by changing several parameters, and discuss the impact of different traffic loads and ad hoc routing protocols when we integrate them with the MARS and E-MARS schemes. Finally, in Section 5.3 some concluding remarks are included.

5.1 Data Transmission Study

In this section, the correctness and effectiveness of the MARS and E-MARS schemes in protecting data transmission in ad hoc networks are evaluated under various types of misbehavior on data. The two types of data dropping misbehavior considered here are the individual dropping and colluded dropping. Since both of the MARS and E-MARS schemes

implement single-path data transmission, they are compared to a pair of DSR-based secure transmission protocols 2ACK [56] and TWOACK [4], which also implement single-path transmission, and the original non-secure DSR single-path transmission system [13] in mobile ad hoc networks. Similar to the E-MARS scheme being an enhancement of the MARS scheme, the 2ACK scheme is a modification of the TWOACK scheme. The performance of the proposed schemes is evaluated by means of simulation.

5.1.1 Simulation Methodology

In the simulations, we use the GloMoSim [96] library-based simulator. There are 50 nodes placed randomly within a 1200-meter×1200-meter area. Each node has a radio power range of 376 meters. The channel capacity is 2Mbps. The timeout value τ at the destination is set to 1.0 second and 8.0 seconds respectively. The IEEE 802.11 DCF is used as the MAC layer protocol in the network.

In the simulation, each node is assumed to move independently in the random waypoint model with the same average speed. The minimum and maximum speeds of node movement are 0m/s and 20m/s respectively. Three node pause times 0 second, 100 seconds, and 500 seconds, which represent fast, moderate, and slow node mobility, are considered. The sources and destinations of 10 CBR data sessions are chosen uniformly from the nodes in the area. The data packets of size 128 bytes are generated with interval 0.5 second. The percentage of misbehaving nodes in the network is varied from 0 to 40%. Each simulation runs 10 sessions with each of 500 seconds. The simulation parameters are summarized in Table 5.1.

Table 5.1: Simulation parameters of MARS and E-MARS.

Number of nodes	50
Transmission range	378 meters
Simulation area	1200-meter × 1200-meter
Timeout value (s)	1.0, 8.0
Simulation time	500 s
Packet size	128 bytes
Channel capacity	2Mbps
Number of CBR sessions	10
Packets sent interval	0.5 second
Minimum and maximum pause time	0m/s, 20m/s
Pause time (s)	0, 100, 500
Percentage of misbehaving nodes	0, 10, 20, 30, 40

In the 2ACK scheme, the time out value τ at each intermediate node to detect misbehavior on data is set to 0.15 second, the acknowledgement ratio R_{ack} that indicates the fraction of data packets acknowledged with 2ACK packets by the nodes two-hop away from the sender is set to 0.20, and the threshold R_{mis} that determines the allowable ratio of the total number of 2ACK packets missed to the total number of data packets sent is set to 0.85. In the TWOACK scheme, the time out value τ is set to 0.15 seconds and the threshold H_m of maximum allowable missed TWOACK packets is set to 5. H_m and R_{mis} triggers the misbehavior alarm in these two protocols. The above specified simulation parameters for these two protocols are summarized in Table 5.2.

Table 5.2: Specified simulation parameters of 2ACK/TWOACK.

Timeout value (s)	0.15
Acknowledgement ratio, R_{ack}	0.20
Threshold of missed 2ACK, R_{mis}	0.85
Threshold of maximum allowable missed TWOACK, H_m	5

The implemented single path routing algorithm is an optimized DSR [13]. The DSR protocol has been described briefly in Chapter 4. Please refer to [13] for more details of the DSR protocol. The DSR-based multipath routing algorithm is described in Chapter 4. In the MARS scheme, it is assumed that the correctness of the discovered connectivity information is guaranteed in all cases.

5.1.2 Simulated Scenarios

The following three scenarios are simulated to illustrate the efficiency of the proposed MARS and E-MARS schemes in improving the system performance and their effectiveness in detecting and mitigating different types of misbehavior on data in a mobile ad hoc network. There scenarios are:

1. Normal Conditions: under these conditions, there is no misbehaving node in the network. All nodes are behaving well, and no data packet is dropped in the intermediate nodes intentionally.

2. Individual Dropping: under these conditions, the misbehavior nodes along the data transmission paths drop all the received data packets. However, the misbehavior nodes are not aware of each other and do not cooperate with each other in forming misbehavior.

3. Colluded Dropping: under these conditions, the misbehavior nodes in the network are aware of each other. When two misbehaving nodes are connected with each other along a data transmission path, the first misbehaving node forwards all the received data packets to the second misbehaving node, and the second one drops the data packets. This is the type of misbehavior that most of the single-path secure schemes and the overhearing schemes could not tackle.

5.1.3 Performance Metrics

Three metrics are selected to demonstrate the performance of the MARS and E-MARS schemes under different environments. The performance metrics used to evaluate the effectiveness of MARS and E-MARS schemes are:

1. Data Receive Rate (DRR): this is the ratio of the total number of data packets received at all the destinations to the total number of data packets sent by all the sources in the network. This metric demonstrate the correctness of the schemes in protecting data transmission under different scenarios.

2. Bandwidth Cost for Data (BCD): this is the ratio of the total number of data packets transmitted by all the nodes, including the sources and the intermediate nodes, to the total number of data packets received at all the destinations in the network system. This metric shows the cost for data transmission in the network.

3. Average End-to-end Delay (AED): this is the result obtained through averaging the total end-to-end delay in the system over all the surviving data packets for each source/destination pair. This value includes queuing delays, route discovery delays, retransmission delays at the MAC layer, and propagation delays. This metric illustrate the efficiency of the protocols.

5.1.4 Simulation Results

The simulation results of the compared protocols under various scenarios are presented in this subsection. The results are presented according to normal, individual dropping, and colluded dropping conditions. The performance of the protocols will be discussed in detail in the next subsection.

1. Normal Conditions: Table 5.3 shows the performance of five compared protocols under normal conditions where there is no misbehaving node in the network. The node pause times of 0 second, 100 seconds, and 500 seconds are considered. The timeout value τ at the destination to detect misbehavior on data is 1.0 second here. The MARS and E-MARS provide higher data receive rates than DSR, 2ACK, and TWOACK protocols at all the three pause times tested. They also pay less bandwidth cost for data transmission in the network than the other protocols at all cases. The overhead for our two protocols is that they incur higher end-to-end delay when the nodes in the network move more frequently. The E-MARS protocol provides better delay performance than MARS. This matches with our intention for proposing such an enhancement.

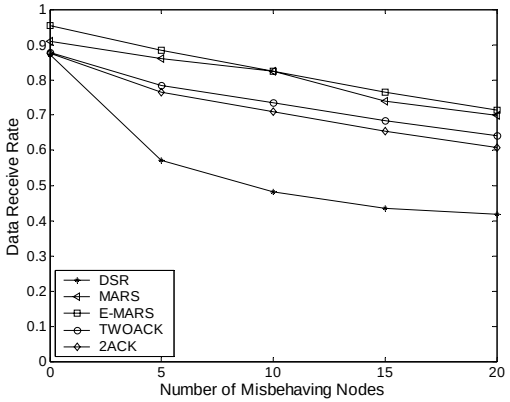
Table 5.3: Performance of compared protocols under normal conditions.

Metrics	Pause time (second)	DSR	TWOACK	2ACK	MARS	E-MARS
Data receive rate	0	0.87	0.878	0.876	0.909	0.955
	100	0.855	0.858	0.857	0.909	0.954
	500	0.863	0.921	0.889	0.938	0.974
Bandwidth cost for data	0	2.579	2.526	2.55	2.339	2.308
	100	3.07	3.025	3.037	2.632	2.622
	500	3.554	3.15	3.396	2.856	2.803
Average end-to-end delay	0	0.01	0.015	0.012	0.05	0.045
	100	0.013	0.022	0.014	0.049	0.034
	500	0.016	0.022	0.017	0.021	0.019

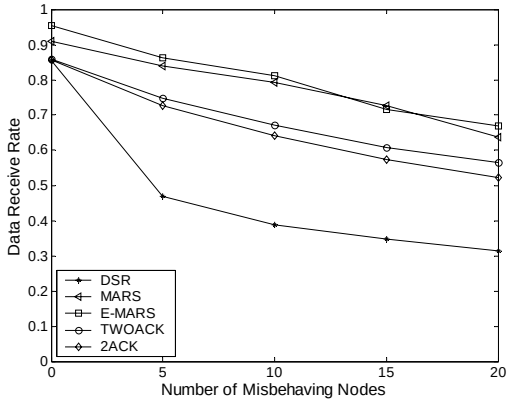
2. Individual Dropping: to demonstrate the performance of MARS and E-MARS on detecting the most-commonly discussed misbehavior against which most of the other protocols aim at defending, we compare them to DSR, 2ACK, and TWOACK under the individual dropping conditions. Figure 5.1 shows the data receive rates of the compared protocols under different node pause times. With the increase of the percentage of misbehaving nodes in the network, the MARS and E-MARS schemes guarantee the data reception and always provide the highest data receive rate in the system under all three cases. The 2ACK and TWOACK also can

guarantee the data reception in the network to some extent but not as good as our two proposed protocols. The data receive rate of DSR decreases dramatically with the increase of misbehaving nodes in the network. Figure 5.2 shows the bandwidth cost for data of the compare protocols under different node pause times. The MARS and E-MARS consume the lowest bandwidth among all the compare protocols. With the increase of the percentage of misbehaving nodes in the network, the cost for DSR increases very fast, especially when the nodes in the system are relatively static. The bandwidth cost for data of 2ACK and TWOACK are between those of DSR and our protocols. The simulation results of these two performance metrics for all the compared protocols when the timeout value τ at the destination is set to 8.0 seconds have not much difference with those when the value of τ is set to 1.0 seconds. Hence, we do not present the simulation results for τ = 8.0 seconds cases.

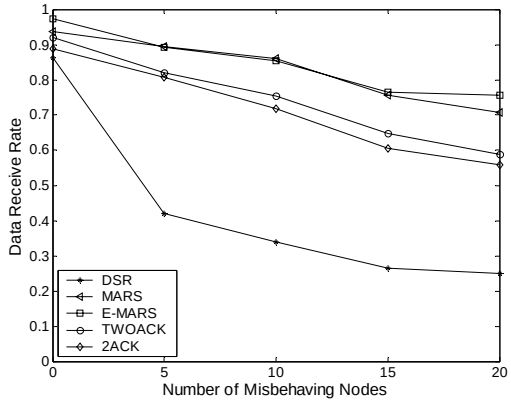
Figure 5.3 shows the average end-to-end delays of the compared protocols with different pause times of the nodes in the network. Our proposed protocols operate with higher delays than the other protocols, among which DSR operates with the lowest delays. However, with the decrease of the node mobility in the system, the delays of our proposed protocols get closer to those of DSR, and the delay differences among the compared protocols get smaller. The simulation results of average end-to-end delay in the network would be different when the timeout value τ at the destination is set to different values. Figure 5.4 shows the comparison of DSR, 2ACK, and our protocols with τ being set to 1.0 second and 8.0 seconds under the conditions of the node pause time being set as 0 second and 500 seconds. A larger value of τ leads to larger delays in the system for MARS and E-MARS, especially when there are a large percent of misbehaving nodes in the network and the nodes in the network are relatively static.



(a) Pause time = 0 second.

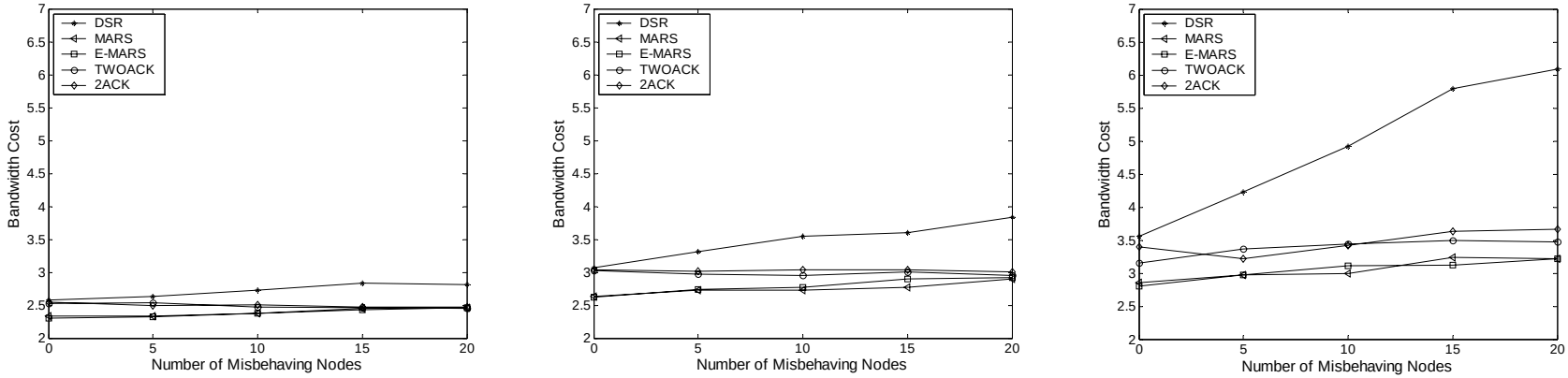


(b) Pause time = 100 seconds.



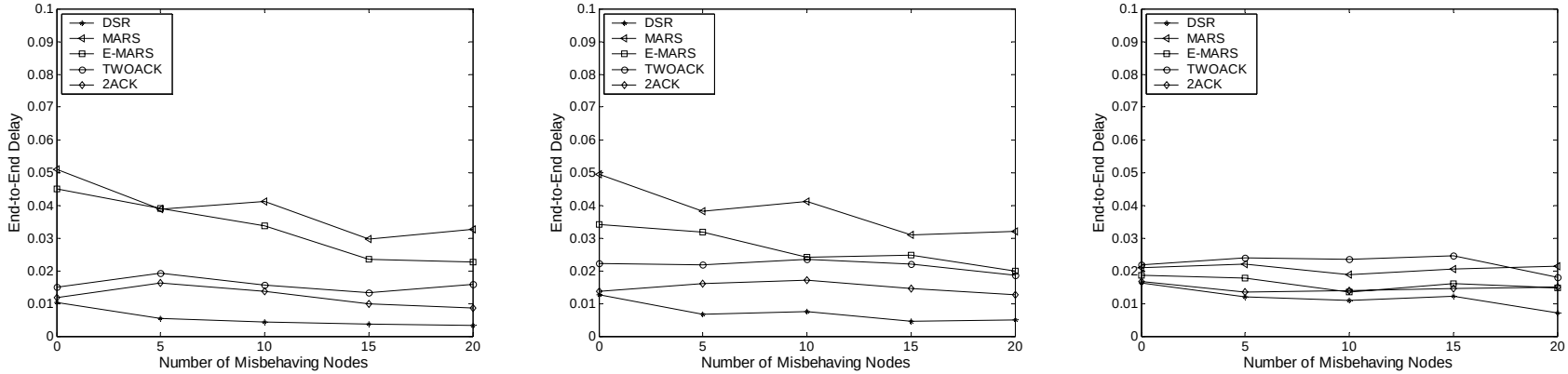
(c) Pause time = 500 seconds.

Figure 5.1: Data receive rates of compared protocols with different pause times under individual dropping.



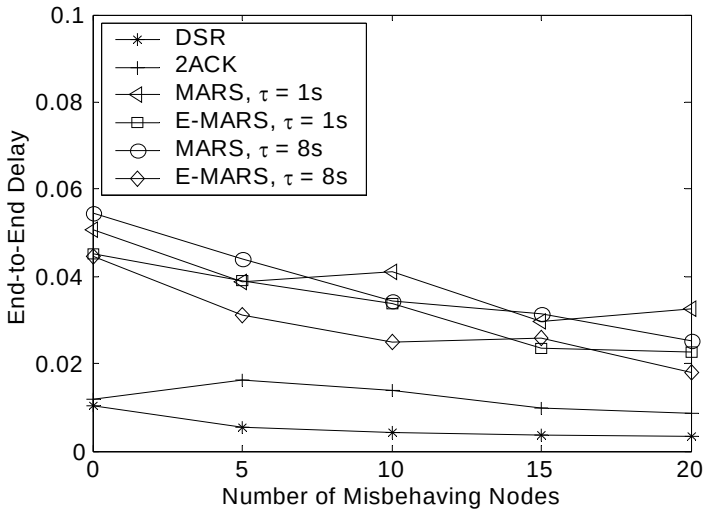
(a) Pause time = 0 second. (b) Pause time = 100 second. (c) Pause time = 500 second.

Figure 5.2: Bandwidth costs for data of compared protocols with different pause times under individual dropping.

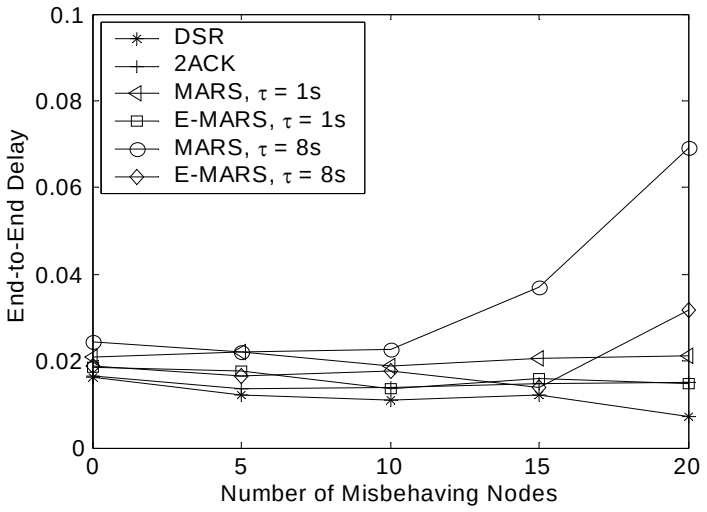


(a) Pause time = 0 second. (b) Pause time = 100 second. (c) Pause time = 100 second.

Figure 5.3: Average end-to-end delays of compared protocols with different pause times under individual dropping.



(a) Pause time = 0 second.



(b) Pause time = 500 seconds.

Figure 5.4: Comparison of delays for different values of the timeout τ at the destination under individual dropping.

3. Colluded Dropping: we also compare the MARS and E-MARS schemes with DSR, 2ACK, and TWOACK under only the colluded dropping conditions. Figure 5.5 shows the data receive rates of the compared protocols under different node pause times. With the increase of the percentage of misbehaving nodes in the network, the MARS and E-MARS schemes guarantee the data reception and keep the data receive rate in the system almost constant under all three cases. All of the DSR, 2ACK, and TWOACK cannot guarantee the data reception in the network. Figure 5.6 shows the bandwidth cost for data of the compare protocols under different node pause times with colluded dropping misbehavior. The MARS and E-MARS consume the lowest bandwidth among all the compare protocols. The cost for DSR, 2ACK, and TWOACK are very close to each other and higher than that of ours, especially when the nodes in the network are relatively static. The simulation results of these two performance metrics for all the compared protocols when the timeout value τ at the destination is set to 8.0 seconds have not much difference with those when the value of τ is set to 1.0 seconds. Hence, the same as under individual dropping misbehavior, we do not present the simulation results for τ = 8.0 seconds cases.

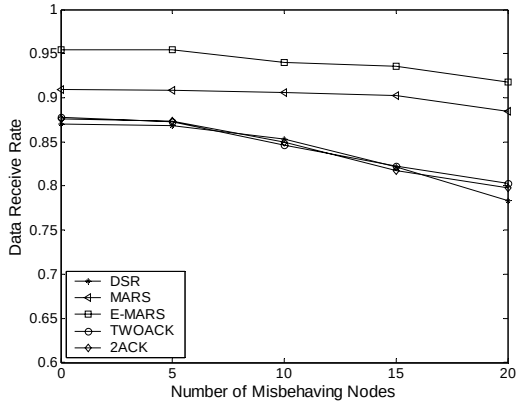
Figure 5.7 shows the average end-to-end delays of the compared protocols with different pause times for network under colluded dropping misbehavior. Similar as under individual dropping conditions, our proposed protocols operate with higher delays than the other protocols, among which DSR operates with the lowest delays. And with the decrease of the node mobility in the system, the delays of our proposed protocols get closer to those of DSR, and the delay differences among the compared protocols get smaller. Figure 5.8 shows the comparison of DSR, 2ACK, and our protocols with τ being set to 1.0 second and 8.0 seconds under the conditions of

the node pause time being set as 0 second and 500 seconds. Different with individual dropping conditions, the simulation results of average end-to-end delay in the network do not have much difference when the timeout value τ at the destination is set to different values.

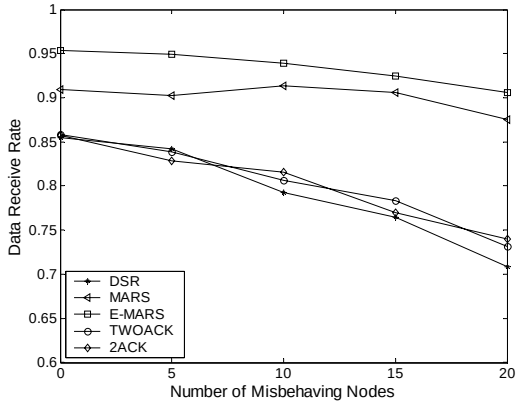
5.1.5 Performance Analysis

In this subsection, we discuss and analyze the performance of the MARS and E-MARS protocols based on the simulation results presented in the above subsection. The multipath routing algorithm makes the nodes have more information about the current network topology and get more fresh paths between each end pair. As one of two selected node-disjoint paths is used for data transmission in the protocols, the data traffic is distributed more evenly in the network. Hence, when all nodes are benign, the MARS and E-MARS protocols have higher data receive rates and lower bandwidth costs for data than the 2ACK, TWOACK, and DSR transmission systems which implement single-path routing.

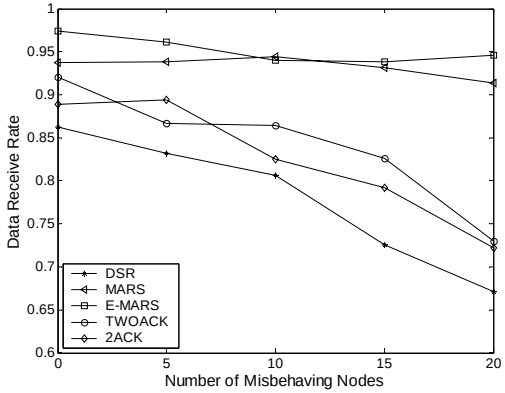
On the other hand, when all nodes are benign, in 2ACK, TWOACK, and DSR the paths used for data transmission are the shortest path in the route cache. The data transmission paths of the two selected node-disjoint paths in our protocols are generally longer than the shortest ones in the route cache. Therefore, the average end-to-end delay in MARS and E-MARS under normal conditions is higher than those of other protocols. Due to the delay-reducing mechanism in E-MARS, the delay of E-MARS is smaller than that of MARS. The simulation results prove that our protocols can provide better system performance than others in a network without misbehaving nodes.



(a) Pause time = 0 second.

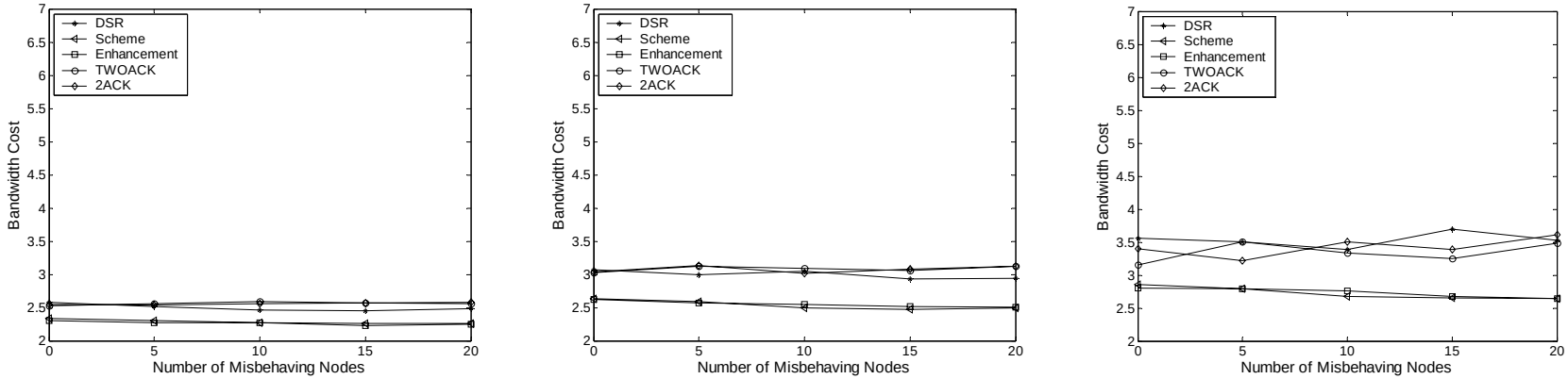


(b) Pause time = 100 seconds.



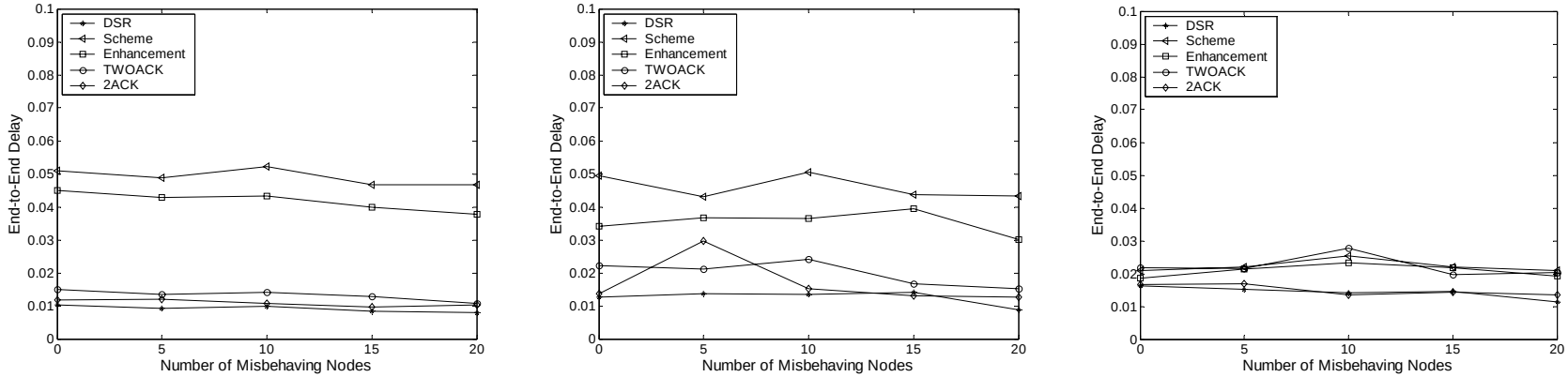
(c) Pause time = 500 seconds.

Figure 5.5: Data receive rates of compared protocols with different pause times under colluded dropping.



(a) Pause time = 0 second. (b) Pause time = 100 seconds. (c) Pause time = 500 seconds.

Figure 5.6: Bandwidth cost for data of compared protocols with different pause times under colluded dropping.

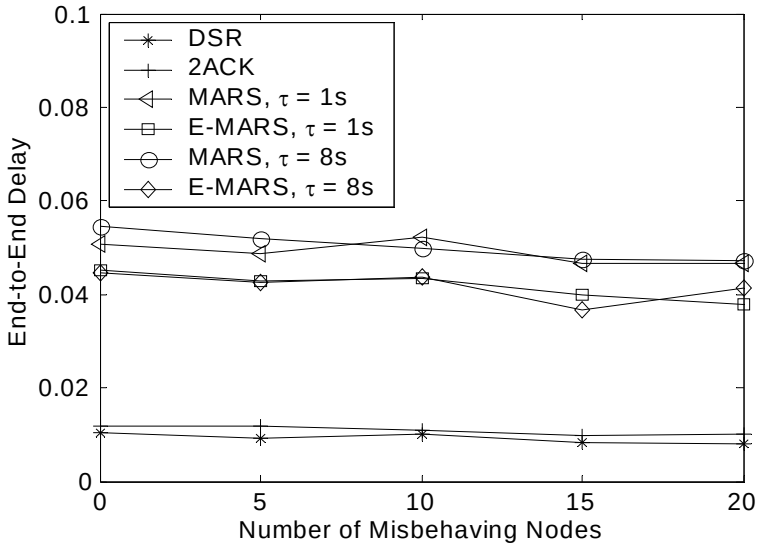


(a) Pause time = 0 second.

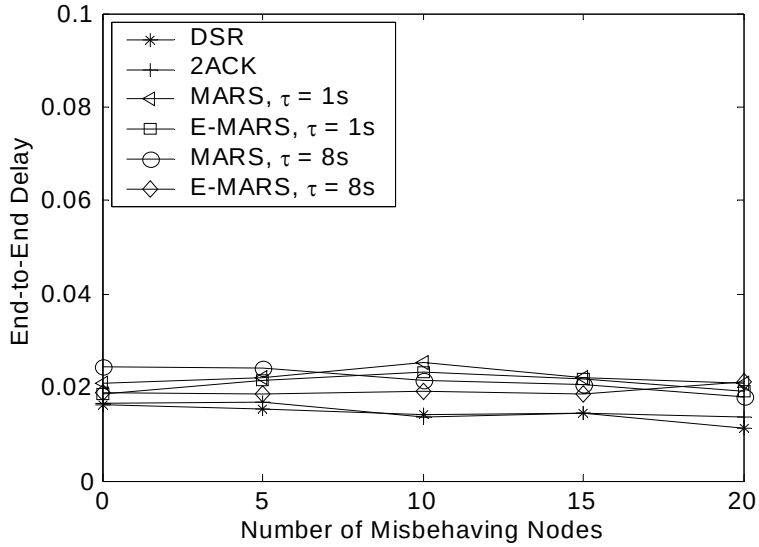
(b) Pause time = 100 seconds.

(c) Pause time = 500 seconds.

Figure 5.7: Average end-to-end delay of compared protocols with different pause times under colluded dropping.



(a) Pause time = 0s.



(b) Pause time = 500s.

Figure 5.8: Comparison of delays for different values of the timeout τ at the destination under individual dropping.

As shown in Figure 5.1 and Figure 5.5, the MARS and E-MARS schemes provide more protection to the data communication under both adverse environments. The data receive rate in the network decreases as the number of misbehaving nodes increases. With pause time 500 seconds and 20% misbehaving nodes in the network, the data receive rate of DSR decreases more than 50% under individual dropping and 8% under colluded dropping. Under the same conditions, the data receive rates of the MARS and E-MARS decrease only around 7% and 1% respectively. The MARS and E-MARS deliver about 90% data packets while DSR delivers only 34%. Even with 40% misbehaving nodes in the network, the data receive rates of MARS and E-MARS are about 50% higher under individual dropping and about 28% higher under colluded dropping than those of DSR. The pair of MARS and E-MARS provides similar protection for data transmission with the pair of TWOACK and 2CK schemes under individual dropping. They outperform the TWOACK and its modified version 2ACK due to the multipath routing mechanism. As the 2ACK and TWOACK have no mechanism to detect colluded dropping, their DRRs decrease just like those of DSR with the increase of misbehaving nodes in the network under such misbehavior.

Figure 5.2 and Figure 5.6 indicate that the DSR, the 2ACK, and the TWOACK have higher bandwidth cost for data compared to the performance of the MARS and E-MARS schemes. With the decrease of node mobility, the bandwidth cost for data of DSR increases dramatically.

As two node-disjoint paths are needed to start the data transmission and the data transmission path may not be the shortest one in source cache, the average end-to-end delays of our MARS and E-MARS are higher than those of the DSR, 2ACK, and TWOACK, as shown in Figure 5.3 and Figure 5.7. Since the MARS needs two node-disjoint paths before the start of data

transmission, it has the highest delays. The E-MARS has lower delays as expected. This is the moderate overhead due to multipath routing. Lower node mobility corresponds to lower route refresh frequency and less buffering time of data packets in the source. The delays of the MARS and E-MARS are quite close to those of DSR, 2ACK, and TWOACK when pause time is 500 seconds.

To investigate the impact of timeout parameter on the network performance, two values of τ, 1 second and 8 seconds, are tested under various adverse environments. As shown in Figure 5.4 and Figure 5.8, different values of τ make different AEDs of the proposed schemes mainly when there is a high percentage (> 30%) of misbehaving nodes in a slow mobile network under individual dropping.

The simulation results show that the MARS and E-MARS schemes are more suitable for slow mobile ad hoc networks. In such a network, they provide significant protection to data transmission with neglectable overhead.

5.2 Detailed Study

The performance of MARS and E-MARS protocols also relates to the other factors such as traffic load in the network and the employed underlying multipath routing algorithms. In this section, we present a detailed study of the impact of routing protocols and traffic load based on simulation results. To mitigate the effect of misbehavior on the system performance, only normal conditions, i.e. no misbehaving nodes in the network, are considered here. The investigated performance metrics are still data receive rate, bandwidth cost for data, and average end-to-end

delay in the system. As only under normal conditions are considered, MARS and E-MARS are compared with DSR in this section.

5.2.1 Impact of Traffic Load

Due to the limitation of wireless channel and implemented MAC protocols, just as it has been shown in Chapter 3 through the analytical models, the performance of data transmission systems in a wireless network relates closely to the traffic load in the system. To investigate the impact of traffic load on our protocols, another set of simulations under heavy traffic load has been executed. The simulation parameters of these experiments are summarized in Table 5.4.

The comparison simulation results of the three performance metrics for DSR, MARS, and E-MARS under normal conditions are presented in Table 5.5. In the case of heavy traffic, there are 4 times of CBR sessions and the 4 times of packet size as those for light traffic case. More nodes contend for the channel and the holding time of the channel for one node is longer. Under such situations, DSR, which uses the shortest paths for data transmission, gives out the highest data receive rate. Unlike under the light traffic cases, MARS and E-MARS deliver fewer packets since the selected paths for data are generally longer than the shortest ones in the route caches of sources.

The bandwidth cost for data of the compared protocols are very close to each other while that of DSR is a little smaller than those of MARS and E-MARS. Due to heave traffic load, the benefit of distributing the traffic evenly in the network becomes less significant for the system performance. The competition for channel becomes fierce in the whole network area.

Table 5.4: Simulation parameters of heavy traffic load.

Number of nodes	100
Transmission range	378 meters
Simulation area	1200-meter × 1200-meter
Packet size	512 bytes
Channel capacity	2Mbps
Number of CBR sessions	40
Packets sent interval	0.5 second
Minimum and maximum pause time	0m/s, 20m/s

The average end-to-end delays of MARS and E-MARS are much higher than those of DSR under heavy traffic cases, while these delays of DSR are higher than those under lighter cases. This indicates that the time searching for node-disjoint paths, contending for channel, and waiting for channel release increases very fast when the traffic load in the network increases.

From the simulation results shown in Table 5.5 and the above analysis, we can see that the MARS and E-MARS are much suitable for a wireless transmission system with light traffic load.

Table 5: Comparison of simulation results of DSR and MARS under different traffic loads.

Metrics	Pause time (second)	Light Traffic			Heavy Traffic		
		DSR	MARS	E-MARS	DSR	MARS	E-MARS
Data receive rate	0	0.87	0.909	0.955	0.958	0.673	0.697
	100	0.855	0.909	0.954	0.962	0.706	0.721
	500	0.863	0.938	0.974	0.979	0.803	0.83
Bandwidth cost for data	0	2.579	2.339	2.308	1.37	1.372	1.379
	100	3.07	2.632	2.622	1.447	1.466	1.447
	500	3.554	2.856	2.803	1.512	1.542	1.528
Average end-to-end delay	0	0.01	0.05	0.045	0.029	1.183	1.528
	100	0.013	0.049	0.034	0.031	1.548	1.635
	500	0.016	0.021	0.019	0.031	2.268	1.621

5.2.2 Impact of Routing Protocol

Our MARS and E-MARS protocols can work above any routing algorithms that can establish at least two node-disjoint paths from the source to the destination. A more efficient multipath routing algorithm can help the proposed protocols demonstrate more benefits. In this subsection, we focus on investigating the impact of underlying multipath routing algorithms on the

performance of these two protocols. The on-demand multipath protocol and the optimized DSR with multipath routing mechanisms that have been described in detail in Chapter 4 are considered here. The performance of DSR, MARS above optimized DSR, as well as the performance of MARS and E-MARS above on-demand multipath routing are simulated and discussed. The simulation parameters of this set of simulation are summarized in Table 5.4.

Figure 5.9 (a) shows the data receive rates of the compared protocols for different node pause times. It illustrates that the data receive rates of MARS above both multipath routing algorithms and E-MARS are fewer than those of DSR. The data receive rates of the MARS scheme based on two multipath routing algorithms and E-MARS are very close to each other. Figure 5.9 (b) shows that the bandwidth cost of MARS above multipath DSR is about 22% ~ 33% higher than that of DSR. The bandwidth cost of MARS and E-MARS above on-demand multipath algorithm is almost the same as that of DSR for different node pause times.

Figure 5.9 (c) shows that the average end-to-end delays for DSR are the lowest among all the compared systems while the delays for MARS above DSR are the highest for different node pause times. The delays for MARS above on-demand multipath algorithm are much lower than that of MARS above optimized DSR. The delays of E-MARS are lower than those of MARS under the same conditions.

The requirement of two node-disjoint paths in our MARS and E-MARS protocols makes the selected paths for data transmission are not necessarily the shortest ones in the route caches of the source, and thus increases the number of data packets transmitted in the system and the number of nodes involved into the data transmission. Simultaneously, the multipath routing algorithms requires more route searching packets transmitted in the network. These mechanisms

increase the contentions for channel in the system and the collisions during data transmission. The source needs to wait more time for the required paths. Hence, an underlying routing protocol that operates with fewer route searching packets and can establish multiple paths between the end nodes more efficiently would guarantee better performance of our proposed protocols.

Between the two compared multipath routing protocols, the on-demand multipath routing algorithm have mechanisms that would obtain multiple paths between two end nodes with much less control packets. Hence, the performance of MARS above on-demand multipath routing algorithm is much better than that of MARS above optimized DSR, especially for bandwidth cost of data and average end-to-end delay.

The performance analysis demonstrates that there needs to be a tradeoff between the complexity of underline routing algorithms and the performance of the proposed protocols. A more efficient routing protocol can certainly make MARS and E-MARS exhibit their benefits better. It needs to point out that, although the simulation results show that the performance of DSR is better than that of MARS and E-MARS in this section, the DSR does not have mechanisms to deal with misbehavior in the network.

5.3 Summary

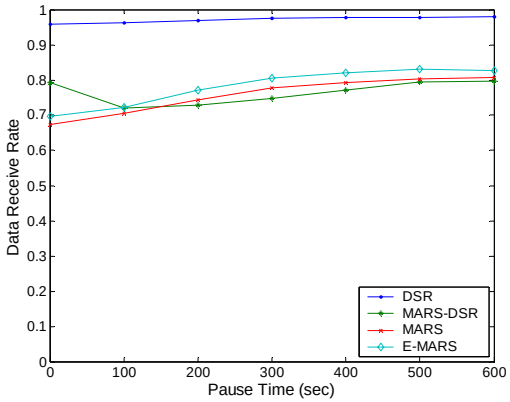
In this chapter, we have analyzed the performance of our proposed MARS and E-MARS protocols for securing data transmission in mobile ad hoc networks by means of simulation under various scenarios. The network performance in terms of data receive rate, bandwidth cost for data, and average end-to-end delay have been examined. The simulation results agree with the analytically design described in the previous chapter. From the simulation results, we can see

that our protocols can provide security protection to data transmission in MANETs while guaranteeing the system performance. The advantage of multipath routing on balancing load in wireless networks is demonstrated in our systems. Another significant advantage of our protocols is that they can detect and mitigate various types of misbehavior on data in the system through the same mechanism. This enables a comprehensive protection to the network system. On the other hand, the performance of our protocols also relate to the timeout parameter at the destination. How to select the optimal timeout value at destination is a topic of future work.

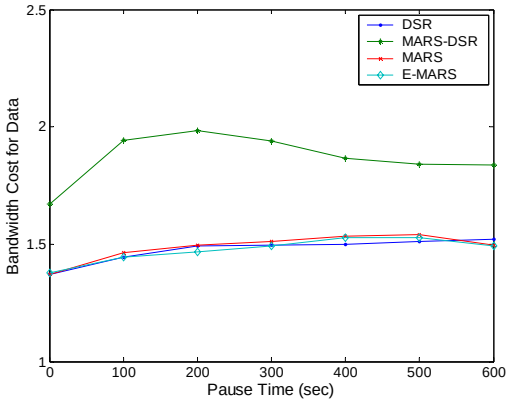
Furthermore, we investigate the impact of traffic load and underlying routing protocol on the system performance by a comprehensive simulation study. The simulation results show that our proposed MARS and E-MARS protocols are more suitable for networks with lighter traffic, and an efficient underlying routing mechanism can help the proposed schemes demonstrate more advantages. Developing multipath routing algorithm more suitable for MARS and E-MARS is another topic of future work.

Our study in this chapter shows that the proposed MARS and E-MARS protocols have the following features:

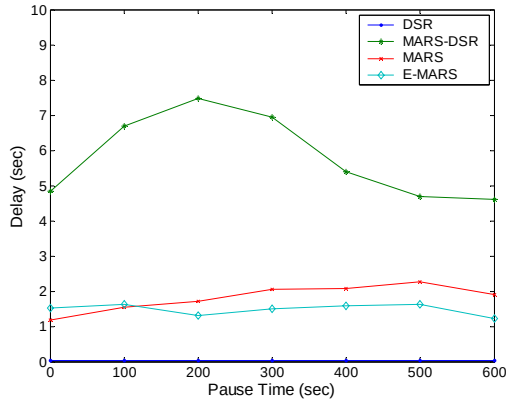
- *Effectiveness*. The MARS and E-MARS effectively detect individual or colluded misbehavior in ad hoc networks.
- *Scalability*. The MARS scheme can be modified to provide further data protection and better network performance. The simple enhancement E-MARS discussed in this paper has convincingly proven this. A reputation system can also be introduced into these schemes.



(a) Packet delivery rate.



(b) Bandwidth cost for data.



(c) Average end-to-end delay.

Figure 5.9: The comparison that shows the impact of underlying routing protocol on the performance of proposed protocols.

Chapter 6

Conclusions

In this dissertation analytical models of multipath multihop transmission system in IEEE 802.11-based wireless networks and two novel protocols for securing data transmission in mobile ad hoc networks have been proposed and evaluated. In this chapter, the major contributions of this dissertation are summarized in Section 6.1 and possible future research directions are discussed in Section 6.2.

6.1 Contributions

The problem of securing data transmission in wireless ad hoc and sensor networks has been considered. As we have reviewed in Chapter 2, most existing security strategies either cannot protect the system from colluded misbehavior or incur much overhead in terms of control message and computing complexity through encryption schemes. Thus, they are not suitable for open MANETs. To fill the gap of these strategies, we have combined the multipath routing and single-path transmission with a robust feedback mechanism to detect misbehavior and mitigate

the adverse effects in mobile ad hoc networks. The protocols are simple, scalable, and capable of protecting the system from individual and colluded misbehavior. Specifically, this research encompasses a variety of analytical and design innovations, including the following:

- *New Analytical Models.* We have developed the analytical models of the frame delay and frame service time at the source as well as the system throughput of multipath data transmission in the IEEE 802.11-based multihop wireless networks. These analytical models are developed from the perspective of interactions between MAC layer protocols and data forwarding at network layer. The models show that the performance of multipath transmission is not necessarily better than that of single-path transmission in 802.11-based wireless networks. The models are validated by means of simulation.

- *Probability of Different Types of Misbehavior based on Analytical Models.* We have built analytical models about the occurrence probability of different types of misbehavior along the data transmission paths in mobile ad hoc networks. The misbehavior could be formed by individual misbehaving nodes or by cooperating misbehaving nodes in the networks. This part of our work is the foundation of our protocols proposed to secure data transmission in MANETs.

- *Novel MARS and E-MARS Protocols.* We have proposed two protocols, MARS and E-MARS, to enhance the security of data transmission in mobile ad hoc networks. They could detect misbehavior on data in the networks and mitigate the adverse effects on network performance. In the proposed protocols, multipath routing mechanism is combined with single-path data transmission and a robust feedback system. The network performance can be guaranteed under normal conditions that all nodes are benign and under various adversarial

environments that misbehaving nodes form misbehavior on transmitted data. The performance of the proposed protocols is evaluated by means of simulation under different scenarios.

It should be pointed out that sybil attack [47], in which a single node presents multiple identities to other nodes in the network, can reduce the effectiveness of multipath routing and may make these schemes fail to work. However, our schemes in combination with other countermeasures, such as radio resource testing, position verification and random key pre-distribution, will be able to defend from sybil attack [65].

6.2 Future Research

Our analytical and simulation results show that MARS and E-MARS can enhance the security of data transmission in mobile ad hoc networks with moderate overhead. However, further work is required to address various properties of MARS and E-MARS. Currently, the basic MARS and E-MARS require a predetermined timeout value τ at the destination for misbehavior detection. As mentioned in Section 4.2, there is no explicit expression of τ. Simulation has to be used to study the effect of a value of τ on the end-to-end delay for a given network scenario (density, mobility, etc.). It would be interesting and useful to find out a way to theoretically get it. In other words, in the future work we are interested in how to theoretically select the optimal value of τ that minimizes the end-to-end delay while guarantees the other performance of the system for a given network scenario.

Another possible interesting topic is to introduce reputation mechanism into the MARS and E-MARS schemes to further enhance the misbehavior detection in the system. As we can see, MARS and E-MARS keep no history record of detected misbehaving paths as well as the

nodes appear on those paths. In a network with high probability of misbehaving nodes, a misbehaving node could appear on selected path after a pervious misbehaving path it is on has been detected. Through introducing a reputation system into the protocols, nodes along the detected misbehaving paths are recorded. A node repeatedly appears on misbehaving paths in a period of time could be identified as misbehaving node and avoid for data forwarding in a duration of future time. This can improve the performance of mobile ad hoc networks with high probability of misbehavior. We have proposed E-MARS as an extension of MARS to improve the performance and our simulation shows that it works quite well. However, there are still possible ways to refine E-MARS and extend MARS.

In this dissertation, we have compared the performance of our proposed protocols with the non-secure single-path DSR as well as the secure single-path 2ACK and TWOACK protocols by means of simulation. We compared the performance of MARS and E-MARS with the multipath transmission secure protocols through the analytical models discussed in Chapter 3. To comprehensively evaluate the performance of MARS and E-MARS, simulation could be used to compare the proposed protocols with some multipath secure protocols, such as SMT.

The simulation study in Chapter 5 shows that the underlying multipath routing algorithm has significant impact on the performance of the proposed schemes. Hence, research on routing protocols suitable for these secure data transmission schemes would be another interesting topic for future work. A multipath routing algorithm that can establish multiple paths between the source and the destination while improving the delay performance of the system is important to MARS and E-MARS.

Bibliography

[1] F. Alizadeh-Shabdiz and S. Subramaniam, "MAC layer performance analysis of multi-hop ad hoc networks," in *Proc. 2004 IEEE Global Telecommunications Conf.*, pp. 2781 – 2785, Nov. 2004.

[2] G. H. Ash, A. H. Kafker, and K. R. Krishnan, "Servicing and real-time control of networks with dynamic routing," *Bell System Technical Journal*, Vol. 60, No. 8, 1981.

[3] E. Ayanoglu, C. I, R. D. Gitlin, and J. E. Mazo, "Diversity coding for transparent self-healing and fault-tolerant communication networks," *IEEE Trans. on Communications*, Vol. 41, No. 11, pp. 1677 – 1686, Nov. 1993.

[4] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: preventing selfishness in mobile ad hoc networks," in *Proc. 2005 IEEE Wireless Communications and Networking Conf.*, pp. 2137 – 2142, March 2005.

[5] C. Balasubramanian and J. J. Garcia-Luna-Aceves, "Shortest multipath routing using labeled distances," in *Proc. the 1st IEEE Int. Conf. on Mobile Ad-hoc and Sensor Systems*, pp. 314 – 323, Oct. 2004.

[6] C. Bao and W. Liao, "Performance analysis of reliable MAC-layer multicast for IEEE 802.11 wireless LANs," in *Proc. 2005 IEEE Int. Conf. on Communications*, pp. 1378 – 1382, May 2005.

[7] Y. Barowski, S. Biaz, and P. Agrawal, "Towards the performance analysis of IEEE 802.11 in multi-hop ad-hoc networks," in *Proc. 2005 IEEE Wireless Communications and Networking Conf.*, pp. 100 – 106, March 2005.

[8] C. Barrett, M. Drozda, A. Matathe, and M. V. Marathe, "Characterizing the interaction between routing and MAC protocols in ad-hoc networks," in *Proc. the 3rd ACM Int. Symposium on Mobile Ad Hoc Networking and Computer*, pp.92 – 103, June 2002.

[9] B. Bellalta, M. Oliver, M. Meo, and M.Guerrero, "A simple model of the IEEE 802.11 MAC protocol with heterogeneous traffic flows," in *Proc. 2005 Int. Conf. on COMPUTER AS A TOOL*, pp. 1830 – 1833, Nov. 2005.

[10] G. Bianchi, “Performance analysis of the IEEE 802.11 distributed coordination function,” *IEEE Journal on Selected Areas in Communications*, Vol. 18, No. 3, March 2000.

[11] G. Bianchi, L. Fratta, and M. Oliveri, “Performance analysis of IEEE 802.11 CSMA/CA medium access control protocol,” in *Proc. 1996 IEEE Int. Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 407 – 411, Oct. 1996.

[12] R. V. Boppana and S. P. Konduru, “An adaptive distance vector routing algorithm for mobile ad hoc networks,” in *Proc. the 20th Conf. of IEEE Communications Society*, pp. 1753 – 1762, April, 2001.

[13] J. Broch, D. Johnson, and D. Maltz, “The dynamic source routing protocol for mobile ad hoc networks,” in http://www.ietf.org/internet-drafts/draftietf-manet-dsr-04.txt, IETF Internet Draft, Nov. 2000.

[14] S. Buchegger and J. L. Boudec, “Nodes bearing grudges: towards routing security, fairness, and robustness in mobile ad hoc networks,” in *Proc. the 10th Euromicro Int. Conf. on Parallel, Distributed and Network-based Processing*, pp. 403 – 410, Jan. 2002.

[15] S. Buchegger and J-Y. L. Boudec, “Performance analysis of the CONFIDANT protocol: cooperation of nodes, fairness in dynamic ad-hoc networks,” in *Proc. the 3rd ACM Int. Symposium on Mobile Ad Hoc Networking and Computer*, pp. 226 – 236, June 2002.

[16] L. Buttyan and J-P. Hubaux, “Enforcing service availability in mobile ad-hoc WANs,” in *Proc. the 1st ACM Int. Symposium on Mobile Ad Hoc Networking and Computer*, pp. 87 – 96, Aug. 2000.

[17] L. Buttyan and J-P. Hubaux, “Stimulating cooperation in self-organizing mobile ad hoc networks,” *ACM/Kluwer Mobile Networks and Applications*, Vol.8, No.5, pp. 579 – 592, 2003.

[18] C. T. Calafate, P. Manzoni, and M. P. Malumbres, “On the interaction between IEEE 802.11e and routing protocols in mobile ad-hoc networks,” in *Proc. the 13th Euromicro Int. Conf. on Parallel, Distributed and Network-based Processing*, pp. 110 – 117, Feb. 2005.

[19] M. Carvallo and J. J. Garcia-Luna-Aceves, “A scalable model for channel access protocols in multihop ad hoc networks,” in *Proc. 2004 Int. Conf. on Mobile Computing and Networking*, pp. 330 – 344, Sept. 2004.

[20] M. M. Carvalho and J. J. Garcia-Luna-Aceves, “Delay analysis of IEEE 802.11 in single-hop networks,” in *Proc. 2003 IEEE Int. Conf. on Network Protocols*, pp.146 – 155, Nov. 2003.

[21] Y.-L. Chang and C.-C. Hsu, "Routing in wireless/mobile ad-hoc networks via dynamic group construction," *ACM Balzer Mobile Networks and Applications Journal*, Vol. 5, pp. 27 – 37, 2000.

[22] C. Chen, W. Wu, and Z. Li, "Multipath routing modeling in ad hoc network," in *Proc. 2005 IEEE Int. Conf. on Communications*, pp.2974 – 2978, May 2005.

[23] C. M. Cordeiro, S. R. Das, and D. P. Agrawal, "COPAS: dynamic contention-balancing to enhance the performance of TCP over multi-hop wireless networks," in *Proc. the 11th Int. Conf. on Computer Communications and Networks*, pp. 382 – 387, Oct. 2002.

[24] H. Deng, W. Li, and D. P. Argawal, "Routing security in wireless ad hoc networks," *IEEE Communications Magazine*, vol. 40, pp.70 – 75, Oct. 2002.

[25] I. F. Díaz, D. Epema, and J. Jongh, "Multipath routing and multiple description coding in ad-hoc networks: a simulation study," in *Proc. the 1st ACM Int. Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks*, pp. 46 – 51, Oct. 2004.

[26] P. E. Engelstad and O. N. Osterbo, "Non-saturation and saturation analysis of IEEE 802.11e EDCA with starvation prediction," in *Proc. the 8th ACM/IEEE Int. Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pp. 224 – 233, Oct. 2005.

[27] Y. Fang and A. B. McDonald, "Cross-layer performance effects of path coupling in wireless ad hoc networks: power and throughput implications of IEEE 802.11 MAC," in *Proc. the 21st Int. Performance Computing and Communications Conf.*, pp. 281 – 290, April 2002.

[28] B. Gaboune, G. Laporte, and F. Soumis, "Expected distances between two uniformly distributed random points in rectangles and rectangular parallelepipeds," *Journal of the Operational Research Society*, vol. 44, no.5, May, pp.513 – 519, 1993.

[29] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *Mobile Computing and Communications Review*, vol. 1, no. 2, pp. 11 – 25, 2001.

[30] B. Ghosh, "Random distances within a rectangle and between two rectangles," *Bulletin of the Calcutta Mathematical Society*, vol.43, pp. 17 – 24, 1951.

[31] R. J. Gibbons, F. P. Kelley, and P. B. Key, "Dynamic alternative routing – modelling and behavior," in *Proc. the 12th International Teletraffic Congress*, 1988.

[32] T. Goff, N. B. Abu-ghazaleh, d. S. Phatak, and R. Kahvecioglu, "Preemptive routing in ad hoc networks," in *Proc. the 7th Annual Int. Conf. on Mobile Computing and Networking*, pp. 43 – 52, July 2001.

[33] N. Gogate, D. Chung, S. S. Panwar, and Y. Wang, "Supporting image and video applications in a multihop radio environment using path diversity and multiple description coding," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 12, no. 9, pp. 777 – 792, Sep. 2002.

[34] Z. Haas, "A new routing protocol for reconfigurable wireless networks," in *Proc. IEEE 6th Int. Conf. on Universal Personal Communications*, pp. 562 – 566, Oct. 1997.

[35] Z. Hadzi-Velkov and B. Spasenovski, "Saturation throughput – delay analysis of IEEE 802.11 DCF in fading channel," in *Proc. 2003 IEEE Int. Conf. on Communications*, pp. 121 – 126, May 2003.

[36] T. Haniotakis, S. Tragoudas, and C. Kalapodas, "Security enhancement through multiple transmission in ad hoc networks," in *Proc. 2004 IEEE Int. Conf. on Communications*, pp. 4187 – 4191, June 2004.

[37] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless ad hoc networks," in *Proc. the 22nd Conf. of IEEE Communications Society*, pp. 1976 – 1986, April 2003.

[38] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. the 4th IEEE Workshop on Mobile Computing Systems and Applications*, pp. 3 – 13, June 2002.

[39] Y.-C. Hu, A. Perrig, and D. B. Johnson. "Ariadne: a secure on-demand routing protocol for ad hoc networks," in *Proc. 2002 Int. Conf. on Mobile Computing and Networking*, pp. 12 – 23, Sep. 2002.

[40] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Efficient security mechanisms for routing protocols," in *Proc. the Network and Distributed System Security Symposium 2003*, pp. 57 – 73, Feb. 2003.

[41] IEEE standard for wireless LAN medium access control (MAC) and physical layer (PHY) specifications, ISO/IEC 8802-11; 1999(E), Aug. 1999.

[42] B. A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T. W. Chen, "Scalable routing strategies for ad hoc wireless networks," *IEEE Journal on Selected Areas of Communications*, Vol. 17, No. 8, pp. pp. 1369 – 1379, Aug. 1999.

[43] N. Jain, D. K. Madathil, and D. P. Agrawal, "Exploiting multipath routing to achieve service differentiation in sensor networks," in *Proc. the 11th IEEE Int. Conf. on Networks*, pp. 681 – 686, Sep. 2003.

[44] P. B. Jeon and G. Kesidis, "Pheromone-aided robust multipath and multipriority routing in wireless MANETs," in *Proc. the 2nd ACM Int. Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks*, pp. 106 – 113, Oct. 2005.

[45] J. Jubin and J. D. Tornow, "The DARPA packet radio network protocols," in *Proceedings of IEEE*, vol.75, no. 1, pp. 21 – 32, Jan. 1987.

[46] J. He, D. Kaleshi, A. Munro, Y. Wang, A. Doufexi, J. McGeehan, and Z. Fan, "Performance investigation of IEEE 802.11 MAC in multihop wireless networks," in *Proc. the 8th ACM/IEEE Int. Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pp.242 – 249, Oct. 2005.

[47] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proc. the 1st IEEE Int. Workshop on Sensor Network Protocols and Applications*, pp. 113 – 127, May 2003.

[48] M. Kefayati, H. R. Rabiee, S. G. Miremadi, and A. Khonsari, "Misbehavior resilient multi-path data transmission in mobile ad-hoc network," in *Proc. the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 91 – 100, Oct. 2006.

[49] Y. B. Ko and N. H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks," *Wireless Networks*, Vol. 6, No. 4, pp. 307 – 321, 2000.

[50] C. K. Lee, X. Lin, and Y. Kwok, "A multipath ad hoc routing approach to combat wireless link insecurity," in *Proc. 2003 IEEE Int. Conf. on Communications*, pp.448 – 452, May 2003.

[51] S. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in *Proc. 2001 IEEE Int. Conf. on Communications*, pp.3201 – 3205, Nov. 2001.

[52] J. Li, C. Blake, D. De Couto, H. Lee, and R. Morris, "Capacity of ad hoc wireless networks," in *Proc. 2001 Int. Conf. on Mobile Computing and Networking*, pp. 61 – 69, July, 2001.

[53] J. Li, Y. Pan, and Y. Xiao, "Performance study of multiple route dynamic source routing protocols for mobile ad hoc networks," *Journal of Parallel and Distributed Computing*, vol. 65, pp. 169 – 177, 2005.

[54] X. Li and L. Cuthbert, "Node-disjointness-based multipath routing for mobile ad hoc networks," in *Proc. the 1st ACM Int. Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks*, pp 23 – 29, Oct. 2004.

[55] H. Lim, K. Xu, and M. Gerla, "TCP performance over multipath routing in mobile ad hoc networks," in *Proc. 2003 IEEE Int. Conf. on Communications*, pp. 1064 – 1068, May 2003.

[56] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgement-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. on Mobile Computing*, 2006.

[57] W. Lou, W. Liu, and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks," in *Proc. the 23rd Conf. of IEEE Communications Society*, pp. 2404 – 2413, March 2004.

[58] J. Macker and S. Corson, "Mobile ad hoc networks (MANET)," IETF WG Charter., http://www.ietf.org/html.charters/manet-charter, 1997.

[59] S. Mao, S. Lin, S. S. Panwar, Y. Wang, and E. Celebi, "Video transport over ad hoc networks: multistream coding with multipath transport," *IEEE Journal on Selected Areas in Communications*, Vol. 21, pp. 1721 – 1737, 2003.

[60] M. K. Marina and S. R. Das, "Ad hoc on-demand multipath distance vector routing," *Wireless Communications and Mobile Computing Special Issue on Wireless Ad Hoc Networks: Technologies and Challenges*, Vol. 6, No. 7, pp. 969 – 988, Oct. 2006

[61] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 2000 Int. Conf. on Mobile Computing and Networking*, pp. 255 – 265, Aug. 2000.

[62] H. Miranda and L. Rodrigues, "Preventing selfishness in open mobile ad hoc networks," in *Proc. the 7th CaberNet Radicals Workshop*, Oct. 2002.

[63] A. Mukherjee, W. Li, and D. P. Agrawal, "Performance analysis of IEEE 802.11 for multi-hop infrastructure networks," in *Proc. 2005 IEEE Global Telecommunications Conf.*, pp. 3439 – 3444, Nov. 2005.

[64] A. Nasipuri, R. Castaneda, and S. R. Das, "Performance of multipath routing for on-demand protocols in mobile ad hoc networks," *Mobile Networks and Applications*, Vol.6, No. 4, pp. 339 – 349, 2001.

[65] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis and defenses," in *Proc. 2004 Int. Symposium on Information Processing in Sensor Networks 2004*, pp. 259 – 268, April 2004.

[66] V-N. Padmanabhan and D-R. Simon, "Secure traceroute to detect faulty or malicious routing," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 1, pp. 77 – 82, Jan. 2003.

[67] V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in *Proc. the 16th Conf. of IEEE Communications Society*, pp. 1405 – 1413, 1997.

[68] C. Perkins and P. Bhagwat, “Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers,” in *Proc. 1994 ACM Conf. on Communications Architectures, Protocols and Applications*, pp. 234 – 244, Aug. 1994.

[69] C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector routing," in *Proc. the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90 – 100, Feb. 1999.

[70] P. P. Pham and S. Perreau, “Performance analysis of reactive shortest path and multi-path routing mechanism with load balance,” in *Proc. the 22nd Conf. of IEEE Communications Society*, pp.251 – 259, April 2003.

[71] P. Papadimitratos and Z. J. Haas, “Secure data transmission in mobile ad hoc networks,” in *Proc. 2003 ACM Workshop on Wireless Security*, pp. 41 – 50, Sep. 2003.

[72] P. Papadimitratos and Z. J. Haas, “Secure routing for mobile ad hoc networks,” in *Proc. 2002 Communication Networks and Distributed Systems Modeling and Simulation Conference*, Jan. 2002.

[73] K. Paul and D. Westhoff, “Context aware detection of selfish nodes in DSR based ad-hoc networks,” in *Proc. 2002 IEEE Global Telecommunications Conf.*, pp.1090 – 3038, Nov. 2002.

[74] M. R. Pearlman, Z. J. Haas, P. Scholander, and S. S. Tabrizi, “On the impact of alternate path routing for load balancing in mobile ad hoc networks,” in *Proc. the 2nd ACM Int. Symposium on Mobile Ad Hoc Networking and Computer*, pp. 3 – 10, Oct. 2001.

[75] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of cooperative black hole attack in wireless ad hoc networks,” in *Proc. 2003 Int. Conf. on Wireless Networks*, pp. 570 – 575, June 2003.

[76] K. Sakakibara, S. Chikada, and J. Yamakita, “Analysis of unsaturation performance of IEEE 802.11 DCF with and without slow contention window decrease,” *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Science*, Vol. E88-A, pp. 2852 – 2862, 2005.

[77] A. P. Santhanam, B. C. Neyveli, and M. Chatterjee, “Traffic diffusion analysis for adaptive multi-path routing algorithm in sensor networks,” in *Proc. 2005 IEEE Global Telecommunications Conf.*, pp.3097 – 3101, Nov. 2005.

[78] K. Stewart, T. Haniotakis, and S. Tragoudas, “A security protocol for sensor networks,” in *Proc. 2005 IEEE Global Telecommunications Conf.*, pp. 1827 – 1831, Nov. 2005.

[79] Y. C. Tay and K. C. Chua, “A capacity analysis for the IEEE 802.11 MAC protocol,” *ACM Wireless Networks*, Vol. 7, pp. 159 – 171, 2001.

[80] O. Tickoo and B. Sikdar, “On the impact of IEEE 802.11 MAC on traffic characteristics,” *IEEE Journal on Selected Areas in Communications*, Vol. 21, No. 3, pp. 189 – 203, Feb. 2003.

[81] O. Tickoo and B. Sikdar, “Queueing analysis and delay mitigation in IEEE 802.11 random access MAC based wireless networks,” in *Proc. the 23rd Conf. of IEEE Communications Society*, pp.1404 – 1413, March 2004.

[82] A. Tsirigos and Z. J. Haas, “Analysis of multipath routing – part I: the effect on the packet delivery ratio,” *IEEE Trans. on Wireless Communications*, Vol. 3, No. 1, pp. 138 – 46,Jan. 2004.

[83] A. Tsirigos and Z. J. Haas, “Analysis of multipath routing – part 2: mitigation of the effects of frequently changing network topologies,” *IEEE Trans. on Wireless Communications*, Vol. 3, No. 2, pp. 500 – 511, Mar. 2004.

[84] A. Valera, W. K. G. Seah, and SV. Rao, “Cooperative packet caching and shortest multipath routing in mobile ad hoc networks,” in *Proc. the 22nd Conf. of IEEE Communications Society*, pp. 260 – 269, April 2003.

[85] L. Venkatraman and P. Agrawal, “Strategies for enhancing routing security in protocols for mobile ad hoc networks,” *Journal of Parallel and Distributed Computing*, Vol. 63, No. 2, pp. 214 – 227, Feb. 2003,

[86] S. Vutukury and J. J. Garcia-Luna-Aceves, “MDVA: a distance-vector multipath routing protocol,” in *Proc. the 20th Conf. of IEEE Communications Society*, pp.557 – 564, April 2001.

[87] Y. Wang and J. J. Garcia-Luna-Aceves, “Modeling of collision avoidance protocols in single-channel multihop wireless networks,” *ACM Wireless Networks*, Vol. 10, pp.495 – 506, 2004.

[88] L. Wang, Y. Shu, M. Dong, L. Zhang, and O. W. W. Wang, “Adaptive multipath source routing in ad Hoc networks,” in *Proc. 2001 IEEE Int. Conf. on Communications*, pp. 867 – 871, Nov. 2001.

[89] W. Wei and A. Zakhor, “Robust multipath source routing protocol (RMPSR) video communication over wireless ad hoc networks,” in *Proc.2004 IEEE Int. Conf. on Multimedia and Expo*, pp. 1379 – 1382, June 2004.

[90] K. Wu and J. Harms, “Performance study of a multi-path routing method for wireless mobile ad hoc networks,” in *Proc. the 9th Int. Workshop on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems*, pp. 99 – 107, Aug. 2001.

[91] H. Wu, Y. Peng, K. Long, S. Cheng, and J. Ma, "Performance of reliable transport protocol over IEEE 802.11 wireless LAN: analysis and enhancement," in *Proc. the 21st Conf. of IEEE Communications Society,* pp. 599 – 607, June 2002.

[92] Y. Xi, J. Wei, and Z. Zhuang, "Throughput analysis of IEEE 802.11 DCF over correlated fading channel in MANET," in *Proc. 2005 Int. Conf. on Wireless Communications, Networking and Mobile Computing*, pp. 694 – 697, Sept. 2005.

[93] Y. Xiao, "Performance analysis of IEEE 802.11e EDCF under saturation condition," in *Proc. 2004 IEEE Int. Conf. on Communications*, pp. 170 – 174, June 2004.

[94] Y. Xue and K. Nahrsted, "Providing fault-tolrant ad-hoc routing service in adversarial environments," *Wireless Personal Communications*, Vol. 29, pp. 367-388, 2004.

[95] Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "A framework for reliable routing in mobile ad hoc networks," in *Proc. the 22nd Conf. of IEEE Communications Society*, pp. 270-280, April 2003.

[96] X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: a library for parallel simulation of large-scale wireless networks," in *Proc. 1998 Workshop on Parallel and Distributed Simulation,* pp. 154-161, May 1998.

[97] H. Zhai, Y. Kwon, and Y. Fang, "Performance analysis of IEEE 802.11 MAC protocols in wireless LANs," *Wireless Communication and Mobile Computing,* pp. 917-931, 2004.

[98] L. Zhang, Z. Zhao, Y. Shu, L. Wang, and O. W. W. Yang, "Load balancing of multipath source routing in ad hoc networks," in *Proc. 2002 IEEE Int. Conf. on Communications*, pp.3197-3201, April 2002.

[99] L. Zhou and Z. J. Haas, "Securing ad hoc networks", *IEEE Network*, pp. 24-30, Nov/Dec 1999.

Appendix

Publications of this Work

This appendix gives a list of papers published and submitted for publication during the course of this research.

[1] Li Zhao, José G. Delgado-Frias, and Krishnamoorthy Sivakumar "Performance Analysis of Multipath Transmission over 802.11-based Multihop Ad Hoc Networks: A Cross-Layer Perspective," accepted by *IET Communications (formerly IEE Proceedings – Communications)*, 2007.

[2] Li Zhao and José G. Delgado-Frias, "MARS: Misbehavior Detection in Ad Hoc Networks," accepted by *the 50th Annual IEEE Global Communications Conference (GlobeCom 2007)*, November 26-30, 2007, Washington, DC.

[3] Li Zhao and José G. Delgado-Frias, "A Multipath Routing-based Misbehavior Detection in Ad Hoc Networks," accepted by *International Conference on Communications and Networking in China (ChinaCom 2007)*, August 22-24, 2007, Shanghai, China.

[4] Li Zhao and José G. Delgado-Frias, "On Throughput of Multipath Data Transmission over Multihop Ad Hoc Networks," *the IASTED International Conference on Wireless Sensor Networks (WSN 2006)*, July 03-04, 2006, Banff, Canada.

[5] Li Zhao and José G. Delgado-Frias, "Performance Analysis of Multipath Data Transmission in Multihop Ad Hoc Networks," *the 2006 International Workshop on Wireless Ad-hoc and Sensor Networks (IWWAN 2006)*, June 28-30, 2006, New York, NY.

[6] Li Zhao and José G. Delgado-Frias, "Multipath Routing Based Secure Data Transmission in Ad Hoc Networks," *the 2nd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2006),* June 19-21, 2006, Montréal, Canada.

[7] Li Zhao and José G. Delgado-Frias, "An Efficient Scheme against Various Attacks in Ad Hoc Networks," *the 2nd IASTED International Conference on Communication and Computer Networks (CCN 2004),* Nov. 2004, MIT Cambridge, MA.

[8] Li Zhao and José G. Delgado-Frias, "Protect Multiple Attacks in Ad Hoc Networks by Using Diversity Routing," *the 8th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2004),* July, 2004, Orlando, FL.

[9] Jin Ding, Li Zhao, Sirisha Medidi, and Krishna. M. Sivalingam, "MAC Protocols for Ultra-Wide-Band (UWB) Wireless Networks: Impact of Channel Acquisition Time," *the SPIE ITCOM Conference*, 4869, July, 2002, Boston, MA.