PERFORMANCE IMPROVEMENT IN MOBILE AD-HOC NETWORKS

A Dissertation
Presented to
The Academic Faculty

By

Sung Jin Park

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
in
Electrical and Computer Engineering

School of Electrical and Computer Engineering
Georgia Institute of Technology
December 2012

PERFORMANCE IMPROVEMENT IN MOBILE AD-HOC NETWORKS

Approved by:

Dr. John A. Copeland, Advisor
John H. Weitnauer, Jr., Chair
School of ECE
Georgia Institute of Technology

Dr. Yusun Chang, Co-advisor
Adjunct Professor, School of ECE
Georgia Institute of Technology

Dr. David G. Taylor
Professor, School of ECE
Georgia Institute of Technology

Dr. Henry L. Owen
Professor, School of ECE
Georgia Institute of Technology

Dr. Raheem A. Beyah
Professor, School of ECE
Georgia Institute of Technology

Dr. Mostafa H. Ammar
Professor, College of Computing
Georgia Institute of Technology

Date Approved: November 2, 2012

DEDICATION

To my family for their support and encouragement.

ACKNOWLEDGEMENTS

I would like to gratefully and sincerely thank Dr. John A. Copeland for his guidance, understanding, patience, and encouragement during my graduate studies at Georgia Institute of Technology. I still remember vividly when I met him first time on December 2009. He opened his office door with smile and welcomed me. I am also very grateful to my committee members, Dr. David Talyor, Dr. Henry Owen, Dr. Yusun Chang, Dr. Raheem A. Beyah, and Dr. Mostafa Ammar for their invaluable support on my thesis.

My special thanks go to my coadvisor Dr. Yusun for his guidance and support during my study. He has always been available when I needed advice. I wish to express my gratitude to all CSC (Communication Systems Center) members for their excellent advice, constructive criticism, helpful and critical reviews throughout my Ph.D study. (Dr. Raheem A. Beyah , Dr. Selcuk Uluagac, Faisal Khan, Jinyoun Cho, Shi-in Chang, and Moazzam Khan) And I would like to thank Yonghee, Heajoon, Dongsik, Junghee, Mintae, Hobak, and Serhee for being my supporters during my study.

Lastly, I would like to thank my lovely wife Sunyoung and my daughter Seoyeon for their love and support during the past four years. I could not have accomplished my Ph.D study without their love and understanding.

"Thank you for choosing me as your advisor."

from Prof. John A. Copeland, 2009

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

The objective of this research is to enhance the network performance under realistic mobile ad-hoc networks environments without modification of the standard. Overview of this research is summarized as follows:

First, a packet-fragmentation technique to improve network throughput under the worst channel conditions is proposed. While the conventional packet-fragmentation technique research focuses only on random-bit errors, the proposed technique employs both random-bit errors and hidden-node collisions. The analytical models based on Markov-chain model shows that the optimal fragmentation technique can effectively reduce the number of retransmissions caused by both collisions from hidden nodes and corrupted packets by random-bit errors, and eventually improving throughput in noisy VANETs channels.

As a second contribution, a dynamic service-channel allocation (DSCA) scheme is proposed to maximize the network throughput by dynamically assigning different service channels to the users. The theoretical analysis in this thesis will consider wireless access in the vehicular environment (WAVE) protocol, which is the main characteristic of the vehicular ad-hoc networks standard (the IEEE 802.11p).

To summarize, the main contribution of this research is that two schemes will improve the network throughput significantly without modification of the standard. Therefore, there is no implementation issue to deploy the proposed schemes in real devices.

CHAPTER 1

INTRODUCTION

The IEEE 802.11 wireless network, also known as WiFi, has been popular by the use of unlicensed band and inexpensive devices. With the increasing demand for seamless and ubiquitous Internet connectivity, a considerable number of studies have been conducted on the mobile ad-hoc networks over the last decade. The mobile ad-hoc networks (MANETs) are distributed networks, where wireless mobile devices can dynamically self-organize arbitrarily and temporarily (ad-hoc), by allowing devices to connect to each other in areas with no pre-existing communication infrastructure.

As an extension of MANETs research, the IEEE 802.11p standard for vehicular ad-hoc networks (VANETs), which is a subset of MANETs, was finalized in 2010. The main objective of VANETs is to support both vehicle to vehicle communication (V2V) and vehicle to infrastructure (V2I) communication for the passenger's safety and traffic information. Therefore, the momentum of research interest on high mobile (or vehicular) ad-hoc networks has been more accelerated.

The MANETs as well as VANETs use carrier-sense multiple access with collision avoidance (CSMA/CA) to avoid collisions as multiple access method. However, the CSMA/CA protocol has several performance issues such as interference, hidden-node problem, multi-hop problem, and fairness issue. Moreover, the dynamic wireless-channel environment resulting from the node mobility causes severe performance degradation in the network. To meet demands of quality of service and high network throughput in mobile ad-hoc networks, many researchers suggested alternative protocols and algorithms to solve performance issues. However, most of these require protocol modifications that result in the deployment issues in real devices.

1.1 Research Objectives

In this thesis, two algorithms are introduced to enhance the network performance under realistic wireless environments without modification of standards. This work will provide a solid foundation to the research communities in solving performance issues in MANETs as well as VANETs.

First, the optimal packet fragmentation technique is introduced as a primary contribution in this thesis. In real mobile ad-hoc networks (MANETs) environments, the network topology keeps changing dynamically, and retransmissions occur frequently because of unexpected collisions by other nodes in the networks. Besides, when wireless channels experience multi-path fading, obstacles, and interference, a wireless station will suffer from packet drops by random-bit errors. To make matters worse, these collisions and packet drops by random-bit errors occur simultaneously. Numerous ideas have been proposed to reduce the collisions and packet drops by random-bit errors in high mobile wireless environments. However, these solutions not only treated these problems individually, but also required protocol modifications. Hence, the packet-fragmentation technique to improve network throughput under worst channel conditions is proposed in this thesis. Although the conventional packet-fragmentation technique research focuses only on bit-error rates (BERs), the proposed technique will employ random-bit errors as well as hidden-node problem. The analytical model, simulation results, and the experimental results will show that the optimal fragmentation technique can effectively reduce the number of retransmissions caused by both collisions from hidden nodes and corrupted packets from random bit-errors, eventually improving throughput in noisy MANETs channels.

In addition to above problems (packet drops by random-bit errors and unintended collisions), multi-channel allocation, which is how to allocate available channels to the stations efficiently in the network, is also critical to the performance in VANETs. The efficient distribution of mobile nodes over the available channels could contribute to the quality of service (QoS) for the real-time data packets and to emergency messages in VANETs. Numerous algorithms have been suggested to utilize the channel capacity in VANETs. Although providing tools to achieve high level of transportation safety is one of the most important objectives in vehicular ad-hoc networks (VANETs) studies, most of these algorithms share safety message communication resources to achieve channel utilization, which results in system-performance degradation of safety-message dissemination. Moreover, wireless access in the vehicular environment (WAVE) protocol, which is main characteristic of vehicular ad-hoc networks standard (the IEEE 802.11p), cause severe collisions among high access categories in a dense traffic condition. As a second contribution, a dynamic service-channel allocation (DSCA) scheme is proposed to maximize the network throughput by assigning different service channels to the users dynamically. The theoretical analysis will incorporate the WAVE protocol characteristic, thus, the number of collisions among high access categories is reduced dramatically.

1.2 Dissertation Outline

This dissertation is organized into six chapters. Chapter 2 introduces the performance issues in MANETs with general overview of the IEEE 802.11 Standard, specifically discussing medium access control (MAC) layers based on the CSMA/CA protocol. Chapter 3 introduces a packet fragmentation technique with hidden nodes with theoretical analysis using Markov-chain model and extensive simulations using OPNET simulator. Section 3.4 shows the experimental results of packet-fragmentation technique implemented in six laptops (Lenova R400) connected to Orinoco Proxim Gold LAN cards and external antennas for 802.11b ad-hoc mode, examining the network throughput in out-door wireless environment. In Chapter 4, the packet-fragmentation technique incorporating the WAVE protocol is validated under vehicular environments based on the IEEE 802.11p Standard. In this chapter, we also introduce the excessive collision problem among high access categories in vehicular ad-hoc networks. To solve this collision problem, Chapter 5 introduces a dynamic service-channel allocation (DSCA) scheme and the simulation results using NS3 (Network Simulator 3). The concluding remarks and future works are in Chapter 6.

CHAPTER 2

PROBLEM DEFINITION IN MOBILE AD-HOC NETWORKS

The mobile ad-hoc networks (MANETs) are distributed networks that consist of wireless mobile devices interconnected by multi-hop communication. Unlike the conventional wireless networks, MANETs have no pre-existing communication infrastructure, and the mobile nodes can dynamically self-organize arbitrarily and temporarily (ad-hoc).

The mobile ad-hoc networks are based on the IEEE 802.11 medium access control (MAC) as a standard for wireless LANs. The IEEE 802.11 MAC is designed to operate well in wireless environments. In real mobile environments, the performance of high mobile communication depends on the wireless environments, which can be deteriorated by interferences from other devices, path loss, multi-path fading, and unintended collisions. Moreover, large number of nodes could bring congestion in the network, and thus, increase the collision probability remarkably, if they exceed the appropriate channel capacity. In this chapter, the performance-degradation issues and related works in mobile ad-hoc networks (MANETs) will be introduced.

2.1 Overview of the IEEE 802.11 Standard

In the IEEE 802.11 CSMA/CA (Carrier Sensing Multiple Access with Collision Avoidance), medium access control (MAC) uses a distributed coordination function (DCF) as a default. In the distributed coordination function (DCF), stations use a random back-off with the contention-based services. When all mobile stations access to the medium, they sense the channel to determine whether the medium is busy or idle, which is called carrier sensing. If the channel is busy for the transmission of sender, all contending nodes must freeze their back-off counter until the senders complete their transmission. If the channel is idle for more than the DCF inter-frame space (DIFS), the stations start to decrease the back-off counter until the back-off timer expires, and start their transmissions as depicted in Figure 1. Since each node randomly chooses one slot time among the slots in the contention window, the stations could avoid collisions with certain probabilities depending on their current back-off stage.

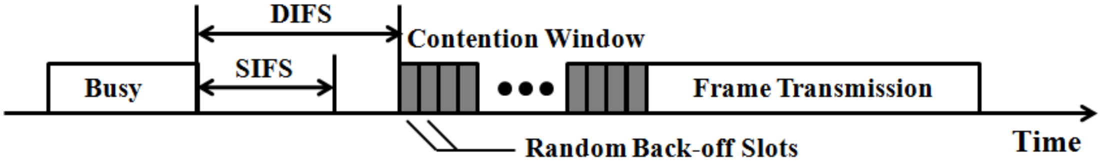


Figure 1: CSMA/CA contention-based service.

For the reliable transmission between the sender and the receiver, a positive acknowledgment (ACK) is used, and all unicast data frames should be acknowledged. If the sender did not receive the corresponding acknowledgment from the receiver, the sender assumes that the transmitted packet is lost and prepares the retransmission.

If the back-off counters expire at the same time in different senders, the different senders start their transmissions simultaneously, which eventually introduces collisions. After each sender detects the collision, it increases current contention-window size as double and prepares the retransmissions up to the retry count as shown in Figure 2. Generally, the initial contention-window size is 32, and the maximum contention-window size is 1024. The retry count is 5 for the control frames and 7 for the data frames. This exponential back-off procedure relieves the collision probability among the contending nodes. If the transmission succeeds, the sender resets the current contention-window size with the initial value.

The sender sets an ACK timeout period when the sender finishes the transmission of the packet. If the sender does not receive an acknowledgment frame within the specified ACK timeout period, the sender assumes that a collision is occurred and goes to the back-off procedures with increased contention-window size as double. The ACK timeout period includes the transmission time of the transmitted packet, propagation time of the transmitted packet, short inter-frame space (SIFS) interval, the transmission time of the ACK, and propagation time of the ACK. If the ACK timeout is shorter than this time, then the sender assumes that the packet has been lost and retransmits the data packet unnecessarily.

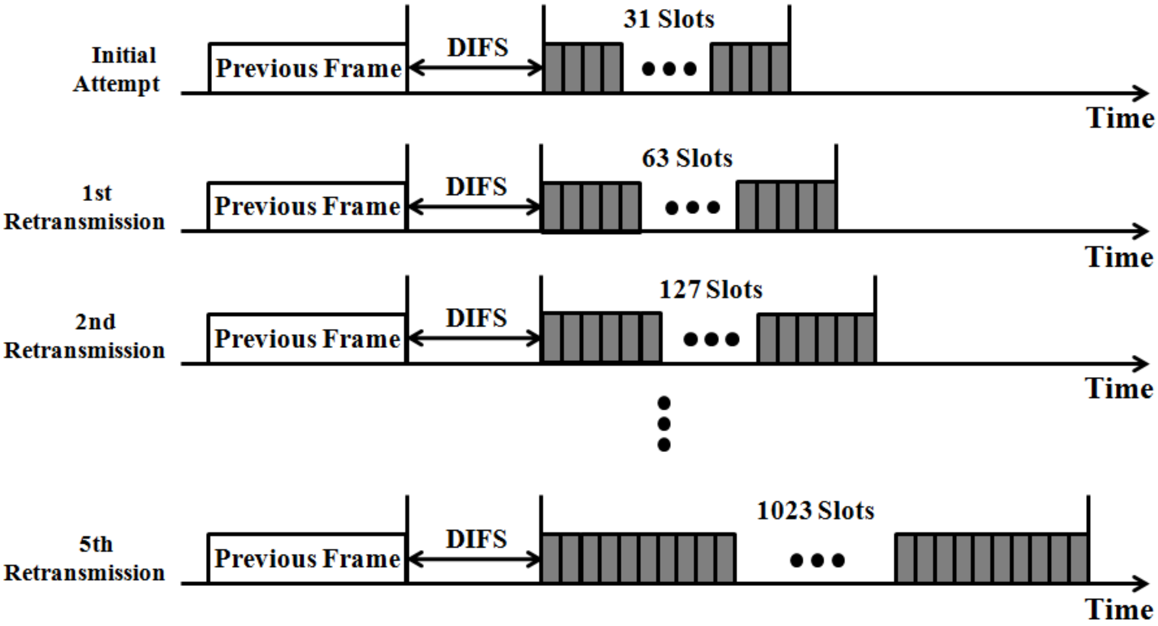


Figure 2: Exponential back-off and retransmission procedure.

However, there is another reason for the unsuccessful transmissions except for the collisions. When the received packet contains errors (called random bit-errors) caused by path loss, multi-path fading, and other reasons in a wireless channel, the receiver cannot decode the packet correctly. Then, the receiver does not transmit the corresponding ACK to the sender, and thus, the sender waits the ACK timeout period and prepares the retransmission. Eventually, the sender increases the current contention-window size unnecessarily.

2.2 Origin and History of the Problem

The highly dynamic network topology in mobile ad-hoc networks compared to the conventional wireless networks causes different wireless environment variations including technical challenges, inefficiency, and limitations. More specifically, in real mobile ad-hoc networks (MANETs), various random-bit errors (BERs) resulting from path-loss, obstacles, and interference cause different probability of successful transmissions. And the frequent collisions by contending nodes in dense traffic condition also reduce the network throughput by wasting the bandwidth for the contention. Lastly, the hidden-node collision is a serious problem in performance degradation. All these parameters have a direct impact on determining the back-off stage of each user during the transmission procedure, since these parameters are connected to the contention-window size. However, most of existing works focus on these parameters separately, which do not provide comprehensive analysis in estimating the performance of the medium access control. In the following subsections, these three problems will be discussed.

2.2.1 Collisions from Contending Nodes

In the IEEE 802.11 MAC, contending nodes can introduce collisions among senders, when their back-off timers expire at the same time. These collisions increase the current contention window by exponential back-off, and thus, change the probability of transmission in a given time slot [1]. Then, the nodes release the channel and go to exponential back-off stage to alleviate the accessibility among contending nodes, which will stabilize the random access medium in 802.11 MAC. When the node density in the network increases, the collision overhead reduces the network throughput drastically. Therefore, the collision probability is critical to the performance evaluation, and the collision probability in CSMA/CA is studied extensively.

The relationship between contention window and exponential back-off is studied by Bianchi [1] to analyze the saturated throughput of the IEEE 802.11 MAC using Markov-chains. One of the main contributions of this model is to provide the probability of transmission of the sender in a given time slot. This probability can be used to derive the probability of collision among the contending nodes. Hence, it can determine the throughput of the network. Based on Bianchi's model, the frame retry count limit is modeled in [2], bit-error rate is included in [3], and the hidden-node problem is investigated in [4]. However, note that as the node has longer waiting time to avoid collisions, the throughput will be deteriorated. In addition, when wireless channels experience multi-path fading, obstacles, and interference, a wireless station will suffer from packet drops because of random-bit errors.

2.2.2 Random-bit Errors

Random-bit error rate (BER) varies widely from many different factors, e.g., modulation techniques, received signal strength, background noise, and interferences from other nodes. The physical layer in the IEEE 802.11 uses different modulation techniques to achieve different data rates. For example, in the IEEE 802.11 DSSS (Direct sequence spread spectrum), the binary phase shift keying (BPSK) is used for 1 Mbps data rate, and complementary code keying (CCK) is used for the data rate 11 Mbps in the IEEE 802.11b. Different data rates (modulation techniques) provide different level of robustness toward noises and interferences.

In addition, the received signal strength is dependent upon the transmission power, multi-path fading, the geometry of terrain, and so on. One of the most efficient statistical measurements for BER is signal to interference plus noise ratio (SINR), which can be used as a mapping tool between the signal at the receiver and its packet-error rate (PER) in the networks. SINR is calculated as the received signal power divided by interference power plus noise power. Hence, the received signal strength is the major factor for the quality of the wireless link.

The IEEE 802.11b and 802.11g use the unlicensed 2.4 GHz ISM (industrial, scientific and medical) band that is vulnerable to the interference from other devices that use the same bandwidth such as microwave ovens and blue tooth devices. Unfortunately, as a user, the only way to resolve the interference problem is to stop using one of the devices [5], which is hard to control in the networks.

When the wireless channel is perfect, the collision caused by contending stations for accessing to the channel will be the only source of unsuccessful transmissions. However, this condition is far from reality, and generally users experience moderate quality channels with contending stations, in which the role of BER becomes more critical in estimating the performance of the networks. Moreover, mobile devices also experience the hidden-node problem which causes another collision in the networks.

2.2.3 Hidden-node Collision

Another factor that causes transmission failures in MANETs is the hidden-node problem, which is an unexpected collision of packets at a receiver sent by senders who cannot sense each other. When a sender starts transmitting its packet, all contending nodes must freeze their back-off counter until the sender completes its transmission. If a hidden node cannot sense the transmission of sender, the hidden node keeps decreasing its back-off counter. When the back-off counter of the hidden node reaches zero, the hidden node starts transmitting packets causing unexpected collisions at the receiver.

Different cases of hidden-node problems are illustrated in Figure 3. A general hidden node case is depicted in Figure 3-a. The hidden node is outside of carrier sensing range of a sender and vice verse. Hence, the hidden-node collision occurs at the receiver. The situation where hidden Node1 and hidden Node 2 are within the carrier sensing boundaries of each other is described in Figure 3-b. Hence, when the hidden Node 1 starts transmitting, hidden Node 2 freezes its back-off counter and does not transmit a packet during the transmission interval of the hidden Node 1. However, the hidden Node 2 in Figure 3-c is also out of the carrier sensing boundary of the hidden Node 1, and it cannot detect the transmission of the hidden Node 1. Then, hidden Node 2 can start its transmission during the transmission of the hidden Node 1. Therefore, the hidden-node effects in Figure 3-b and Figure 3-c can be different. Moreover, the contention-window sizes also could be different in Figure 3-b and Figure 3-c, since the hidden Node 2 is another hidden node to hidden Node 1 in Figure 3-c, whereas the hidden Node 2 is contending node of hidden Node 1 in Figure 3-b. Thus, the contention-window size of hidden nodes could be different in each case, and thus, introduce different collision probabilities.

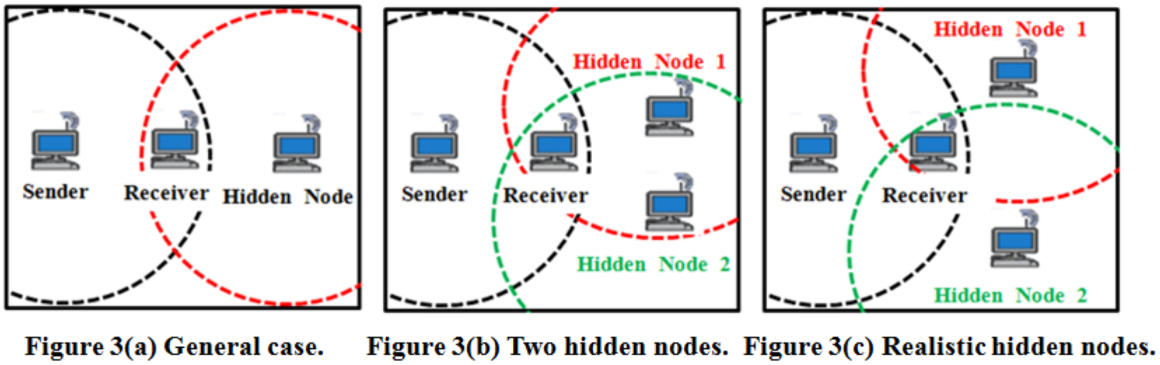

Sender
Receiver
Hidden Node
Hidden Node 1
Hidden Node 2
Figure 3(a) General case.
Figure 3(b) Two hidden nodes.
Figure 3(c) Realistic hidden nodes.

Figure 3: Hidden-node collision examples.

To avoid a hidden-node problem, the RTS/CTS (Request To Send / Clear To Send) mechanism is used in the IEEE 802.11 MAC standard as depicted in Figure 4. The sender broadcasts an RTS control packet that contains the intended destination of the data packet and the amount of channel time required for the transmission in the control field.

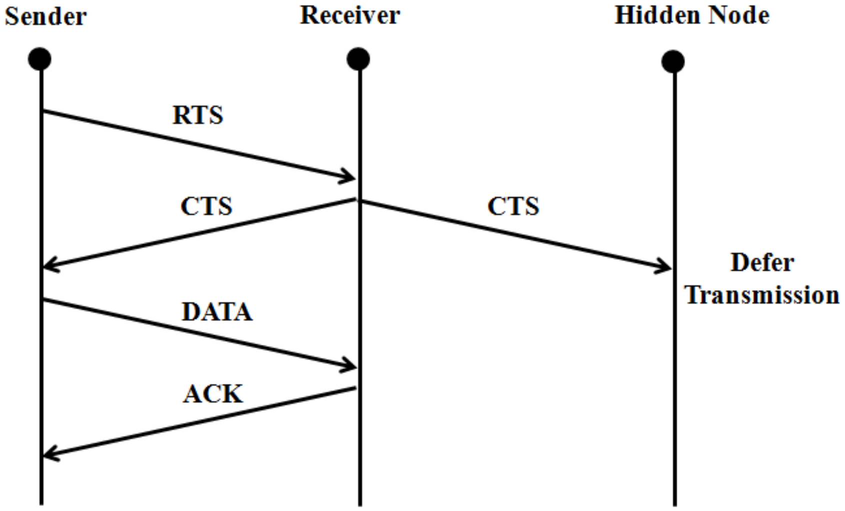


Figure 4: RTS/CTS exchange procedure.

If the RTS packet arrives successfully at the receiver, the receiver broadcasts a CTS control packet that contains the channel time required for the new packet. By replying with the CTS signal, the receiver can inform to the sender that the receiver successfully received the RTS signal. At the same time, the receiver announces to the neighboring stations including hidden nodes specifying the period of transmission time. The neighbor nodes that receive the CTS control signal from the receiver defer their transmission to avoid the collisions.

However, this RTS/CTS mechanism introduces a lot of overheads in transmission time, because every node should exchange the control signals for every data frame. Hence, RTS/CTS mechanism should be recommended for large data frames. Using it for small data frames may result in the significant overhead causing inefficient capacity utilization and higher delays. Generally, channel conditions are not known for users whether hidden terminals exist or not. Therefore, users are forced to decide between either always on or always off in using RTS/CTS, unless some other intelligent algorithm dynamically controls it with estimated or measured channel information, which would also require additional system resources for the estimation or measurement.

Generally, the RTS/CTS mechanism is not suitable for the general ad-hoc networks [6] not only because of that the overheads generated by the RTS/CTS signals degrade the network throughput, but also because of that the RTS/CTS signal exchange also lead some problems as followings:

1. The gagged-station problem [7]: One station wants to receive a packet from other node, when stations are not interfered by any ongoing transmissions. However, the station already received the CTS signals from the receiver, it cannot reply back with CTS signal. For example, there is an ongoing transmission from Node A to Node B as depicted in Figure 5. Node D wants to initiate a transmission to Node C by transmitting RTS signals to Node C, when the transmission between Node D and Node C does not interfere the current transmission from Node A to Node B. Although Node C receives the RTS signal from Node D, it cannot reply back with a CTS signal, because Node C heard the CTS signal from Node B. Hence, the RTS/CTS exchange prevents concurrent transmission, and thus, decreases the entire network efficiency.

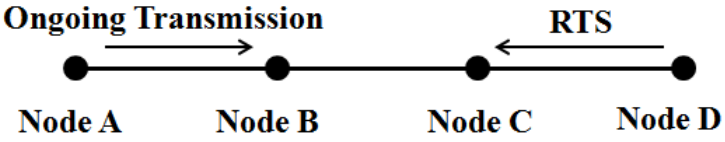


Figure 5: The gagged-station problem.

2. The masked-station problem [8]: Even though the RTS/CTS protocol is designed to solve the hidden-node problem, there still can be collisions of data packets caused by hidden nodes. The reason is that the CTS signal cannot be heard by all neighbor nodes. For example [7], Node D initiates a transmission to Node E in Figure 6. RTS/CTS exchange is finished successfully, and a transmission is ongoing between Node D and Node E. During this transmission, Node A initiates a transmission to Node B by transmitting RTS signal to Node B. When Node B replies back with CTS signal to Node A, Node A can hear it, but Node C cannot hear it because of the ongoing transmission between Node D and Node E. Then, Node C is not blocked by the CTS signal form node B. As soon as Node D completes the transmission, two collision events can be occurred. First, Node C initiates a transmission either Node B or Node D, and the RTS packet from Node C destroys the transmission between Node A and Node B. Second, Node D sends a RTS signal to Node C, and Node C replies back with a CTS signal. This CTS signal destroys the transmission between Node A and Node B. In addition, Node B also cannot hear the CTS signal, and thus, Node B becomes masked (not blocked).

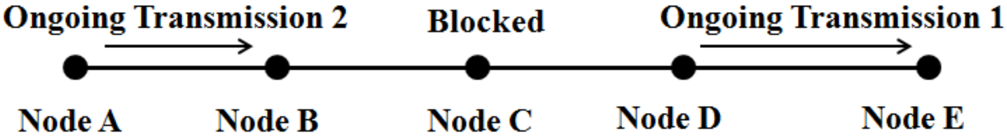


Figure 6: The masked-station problem.

3. The unsuccessful RTS frame transmission : Since every node exchange the RTS/CTS signals after its back-off counter expires, there can be collision between nodes in dense traffic conditions like general packet transmission. In addition, the RTS frame can be corrupted by random-bit errors in noisy wireless environments. In these cases, the RTS signals should be retransmitted, which wastes channel resources. Moreover, when receiver replies back with CTS signal, there could be concurrent RTS frame transmission from other nodes.

Because of these inefficiencies and problems, many researchers proposed other schemes to avoid hidden-node problems, but most of these mechanisms need protocol modifications. The related works on the hidden-node problem will be discussed in the following subsection.

2.3 Related Works

2.3.1 Packet Fragmentation over Random-bit errors (BERs)

The high layer network protocols, for example IP, support the fragmentation method. However, in the network-layer fragmentation, reassembly is performed in the final destination. Hence, if any fragments are lost, the entire packet should be retransmitted [5]. A link-layer fragmentation can be used to boost speed over in a single hop, which means only unsuccessful fragment is retransmitted. The IEEE 802.11 MAC standard supports packet fragmentation in the link layer to avoid the unsuccessful transmissions because of the random-bit errors by burst interference as depicted in Figure 7.

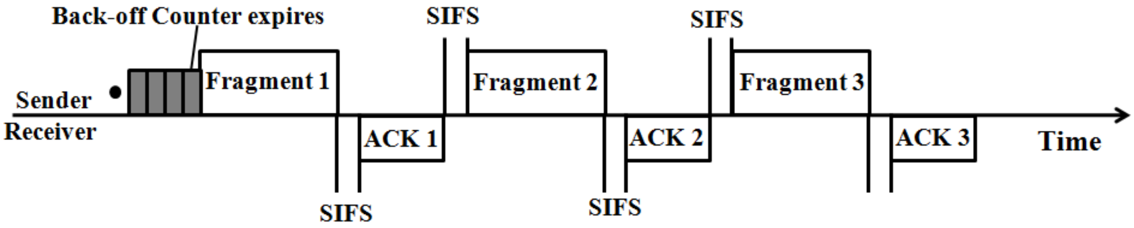


Figure 7: Packet fragmentation.

When a back-off counter is expired, a sender sends the first fragmented packet. The receiver replies back with corresponding ACK after a SIFS interval. To indicate that the next consecutive fragmented packet remains, the frame control field (More Fragments Bits) is set to 1. By doing this, current fragmented packet sets the network-allocation vector (NAV) to lock the medium for the next frames. For the final fragmented frame, a station sets the More-Fragment Bit to 0. There is no limitation for the number of fragmentation frames, but the each fragmented packet length should be longer than the minimum length (256 bytes in the IEEE 802.11b).

If senders break a single packet into smaller fragments, each fragment would have a better chance of escaping the burst packet errors. Therefore, packet fragmentation is one of the most efficient ways to improve the performance without modifying 802.11 MAC protocol.

However, many fragmented packets introduce additional overheads (additional SIFS intervals and ACKs) in transmission time. Moreover, the 802.11 standard leaves the option for selecting optimal fragment lengths to users. Therefore, many research efforts have been made to suggest these optimal packet sizes in [9], [10], [11] and [12] under different channel conditions during last decade. In [9], the authors investigated the optimal packet size with simulations under different BERs, but the authors did not include the packet fragmentation technique. In [10], authors do not provide comprehensive analysis of the network throughput. In [12], a dynamic optimal fragmentation with rate adaptation is proposed. Through the experiments, authors showed that a performance enhancement could be obtained using fragmentation. However, poor channel conditions generally causes not only severe interferences, but also a hidden-node problem, which eventually incurs the performance degradation. Therefore, the detailed behavior of fragmented packets in the existence of hidden nodes needs to be investigated.

2.3.2 Hidden-node Collision

The hidden-node problem is well-known to the wireless networks, since it causes a serious performance degradation. Hence, it has brought attentions to many researchers to investigate the effect of hidden node on the network performance. In [13], the authors derived a mathematical analysis based on queuing theory, and the effect of hidden nodes under saturation condition is investigated in [14] and non-saturation conditions in [**?**]. The performance of the network with hidden nodes is evaluated with the experiments in [8]. These works mostly focused the performance analysis in the network.

Even though RTS/CTS exchange by the IEEE standard can remove the hidden-node problem, many researchers have provided various algorithms to avoid the inefficiencies of the additional overheads caused by the RTS/CTS exchanges, which results in significant performance degradation as discussed in the previous subsection. Moreover, this RTS/CTS exchange could not prevent all the collisions ([6] and [15]), because the control signal can be lost or cannot be decoded correctly [8].

Many researchers suggested solutions for eliminating or reducing the hidden-node collisions instead of the RTS/CTS mechanism. One of the approaches is based on the busy-tone mechanism that was introduced in [16]. The main idea is that a station that is receiving an ongoing transmission sends a busy tone to its neighbors (on a narrow-band radio channel) for preventing them from transmitting during channel use [17]. As extension works, many mechanisms based on the busy-tone mechanism are suggested in [18], [19], and [20]. Nevertheless, these mechanisms need an additional radio channel, and thus, lead to complexity problems and cost problems. The other mechanism [21] and [22] is carrier-sense tuning mechanism in that is extend the detection range of transmission to defer the hidden-node transmission by setting high receiver sensitivity. Some algorithms ([17] and [23]) use different concepts for the solution. The authors in [17] proposed H-NAMe that splits each cluster of a WSN into disjoint groups of non-hidden nodes based on the grouping strategy. Although the strategy is efficient and easy to implement, this approach is only targeting the wireless sensor network without mobility. Most of these researches not only require protocol modification, but also provide little efforts to the verification of proposed models through real-world experiments. Moreover, all above works mainly focus on the hidden node problem, whereas the interference, pathloss, and multipath fading exist as well in general wireless environment. Therefore, we will introduce our technique to solve the hidden-node problem as well as random-bit errors in the next chapter.

CHAPTER 3
PACKET FRAGMENTATION WITH HIDDEN NODES

The main goal of this chapter is to present the optimal packet-fragmentation technique in noisy mobile ad-hoc networks. As introduced in the previous chapter, the hidden-node problem and the random-bit errors (BERs) are serious problems in the network performance. Many research works has conducted on these problems, however, they treat them individually. Generally, users experience the hidden-node collisions as well as packet drops cause by random bit-errors at the same time. Moreover, the existing solutions require protocol modification, which causes deployment issues in real devices. Although packet fragmentation effect over random-bit errors has been investigated by many researchers, this research suggests that the packet fragmentation could have effects not only on the random-bit errors, but also on the hidden-node collisions. This chapter demonstrates a feasible methodology to enhance network throughput in the existence of hidden nodes by using optimal fragments without protocol modifications. The rest of the chapter is organized as follows: In the next section, we introduce the problem and basic idea of the solution. Our system analysis based on the Markov-chain model will be introduced, and the throughput equation will be derived in Section 3.2. We will validate the analytic results with simulation results in Section 3.3, and we will introduce the experimental result in Section 3.4. In the last section, the contributions and challenging problems will be discussed.

3.1 Fragmentation over Hidden-node collision

The optimal packet-fragmentation mechanism focuses on the hostile wireless environments, where the hidden-node collisions occur frequently and the severe interference exists as well. Under these environments, the general transmission procedures without both RTS/CTS handshake and fragmentation in the IEEE 802.11 DCF are depicted in Figure 8. When a received packet contains many random-bit errors caused by burst interference, the receiver cannot decode the data correctly. Hence, numerous retransmission procedures dominate the most of transmission time. Moreover, during the transmission time, a receiver also has vulnerable periods for errors because of hidden-node collisions. In [4], the author mentioned these vulnerable periods for hidden-node collisions with and without RTS/CTS exchanges, and specified the vulnerable periods in terms of back-off slots. If the back-off counter of a hidden node expires during the transmission time of sender, it starts its transmission, since the hidden node cannot sense the packet transmission between the sender and destination. Then, the sender keeps retransmitting the packet up to its maximum retry limit, as a result of the unsuccessful transmissions. Eventually, these retransmissions occupy the entire network bandwidth.

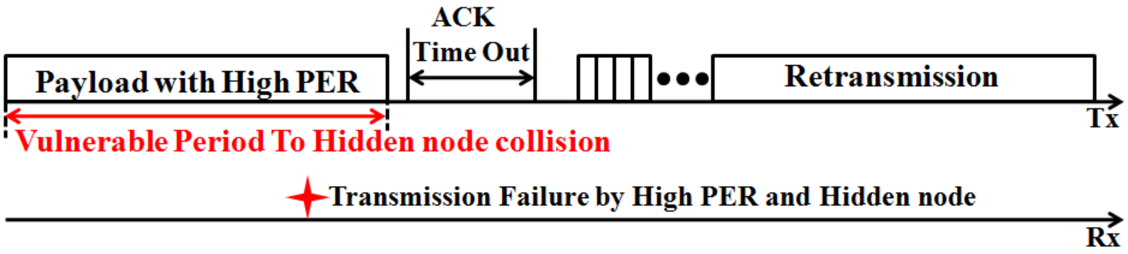

ACK
Time Out
Payload with High PER
Retransmission
Tx
Vulnerable Period To Hidden node collision
Transmission Failure by High PER and Hidden node
Rx

Figure 8: General transmission procedure in noisy wireless channel.

The RTS/CTS exchange mechanism to remove the hidden-node problems is shown in Figure 9. By exchanging RTS/CTS control packets, nodes can avoid collisions caused by hidden nodes, but still they suffer many unsuccessful transmissions resulting from the random-bit errors. Therefore, compared to Figure 8, more overheads for RTS/CTS exchanges are generated (the retransmission of RTS/CTS control signals resulting from random-bit errors), while all the packets are still not delivered successfully to the destination. As mentioned earlier, this RTS/CTS exchange also does not guarantee absolute avoidance of hidden-node collisions.

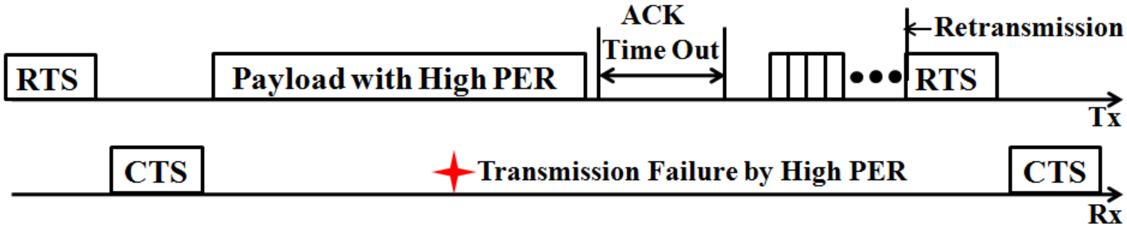


Figure 9: RTS/CTS mechanism in noisy wireless channel.

The packet fragmentation effects on both hidden-node collisions and random-bit errors are illustrated in Figure 10. Because of breaking the long packet into several packets in a high BER channels, the receiver would have a lower packet-error rate (PER). In addition, it would have short vulnerable periods against hidden-node collisions in Figure 10. Therefore, the key idea lies on that an appropriate packet size could decrease both PER and hidden-node collision probability simultaneously by adding small additional overheads for the packet fragmentation.

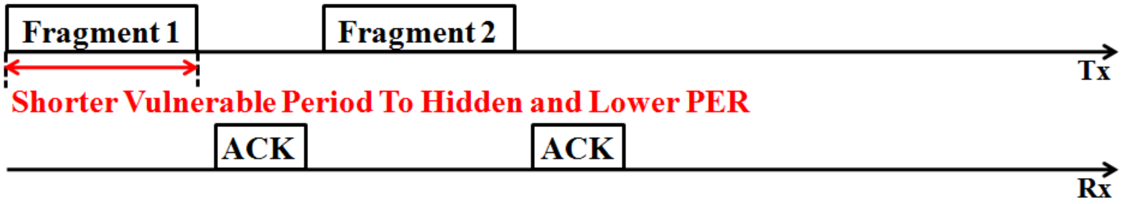


Figure 10: Packet fragmentation in noisy wireless channel.

3.2 System Analysis

3.2.1 Assumption

The IEEE 802.11 medium access control (MAC) analysis [24] is based on the Markov-chain model that is suggested by Bianchi [4], because this model can derive the accurate network throughput equation. However, this model does not include the effect of random-bit errors and hidden nodes. Hence, the probability of hidden-node collision and the unsuccessful transmission probability by BERs are incorporated in our model. The assumptions are as follows: There are several numbers of contending nodes (C_{ni}), and hidden nodes (H_{ni}) in perspective of a sender i (Tx_i). Their corresponding numbers are βi and γi in perspective of a sender i (Tx_i), respectively. Hence, every sender i (Tx_i) has the different number of contending (βi), and number of hidden nodes (γi) regarding on its corresponding destination (Rx_i), and the total number of senders is N. Therefore, the set of senders can be expressed as $\{Tx_1, Tx_2, Tx_3 \ldots\ Tx_N\}$. The set of contending nodes for sender i (Tx_i) can be represented as a set of βi=$\{C_{n1}, C_{n2}, C_{n3} \ldots\ C_{n\beta i}\}$, and a set of hidden nodes for sender i (Tx_i) can be expressed as a set of γi=$\{H_{n1}, H_{n2}, H_{n3} \ldots\ H_{n\gamma i}\}$, respectively. The sender i (Tx_i) could be the hidden node of some senders, the contending node of other senders, since they are competing for the medium access in the network.

3.2.2 Suggested Markov-chain Model

In the Bianchi's Markov-chain model [4], the author defines the probability p as a probability that a transmitted packet collides, and thus, increases current window size to double. This collision occurs when the back-off counters in different contending nodes expire at the same time. However, random-bit error and collisions by hidden nodes can also increase sender's contention-window size even though the sender does not know the exact reasons for transmission failure. This is because of that the IEEE 802.11 MAC is designed for relieving the contention procedures in dense traffic conditions. Thus, if the sender does not receive the corresponding ACK from receiver, the sender assumes that the transmission is failed by the collisions among the contending nodes. To incorporate these two effects, a new modified Markov-chain model is proposed based on the model with maximum retransmission limits [2] as depicted in Figure 11. The $\{s(t),\ b(t)\}$ in Figure 11 represents the state of the station, and the stochastic process representing the back-off window size for a given station at slot time t, respectively [4].

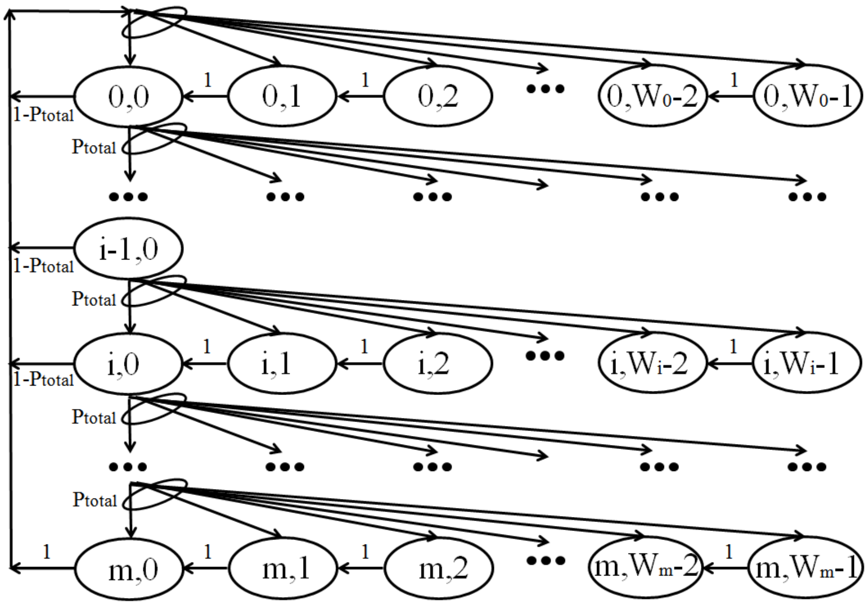


Figure 11: Modified Markov-chain model.

The probability that senders increase the current contention-window size as double can be categorized in three reasons. First reason is the collision by contending nodes, which is the same as in [4]. Second, the collision caused by the hidden nodes. Lastly, the unsuccessful transmission caused by random-bit errors. Therefore, the packet-collision probability on the state $s(t)$ of the station p in [2] is substituted for P_{total} in Figure 11 after incorporating these three probabilities. We also assume that sender i (Tx_i) can transmit a packet with their transmission probability τ_i, where i is from 1 to N. Therefore, the collision probability by contending nodes for sender i (P_{CCNi}) can be represented as

$$P_{CCNi} = 1 - \prod_{P \in \beta i} (1 - \tau_P), \tag{1}$$

while β_i is all sets of contending nodes for sender i, and $(1 - \tau_P)$ means the probability that $Node\,P$ does not send a packet in a given slot time. Even though contending nodes do not send a packet during the transmission time of a sender, there is an another possibility that a collision occurs, when hidden nodes send packets during the transmission time. Because the contending nodes in the same group freeze their back-off counters during the transmission time of a sender, whereas the hidden-node group still continues countdown their back-off counters. In our analysis, the packet transmission time (t_{fk}) means the time period when the sender sends the $k-th$ fragmented packet. Let the MPDU (MAC Protocol Data Unit) size in Figure 12 be L bits and the fragment size be F bits, respectively. Then, the number of fragmented packet (K) of the original MPDU can be expressed as

$$K = \left\lceil \frac{L}{F} \right\rceil . \tag{2}$$

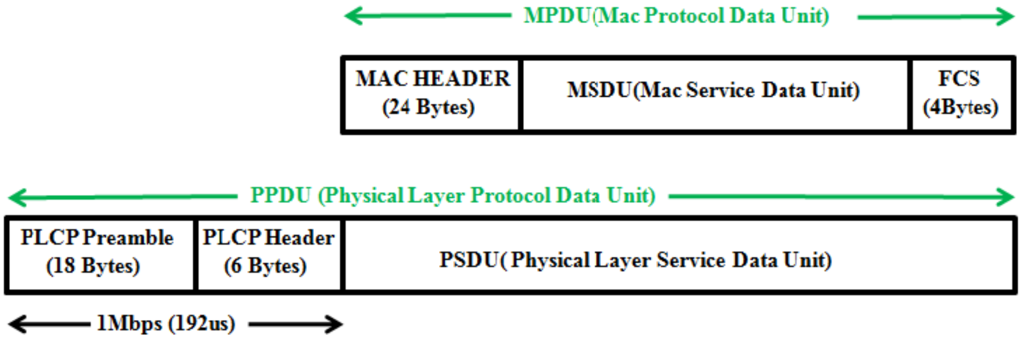

MPDU(Mac Protocol Data Unit)
MAC HEADER (24 Bytes)
MSDU(Mac Service Data Unit)
FCS (4Bytes)
PPDU (Physical Layer Protocol Data Unit)
PLCP Preamble (18 Bytes)
PLCP Header (6 Bytes)
PSDU(Physical Layer Service Data Unit)
1Mbps (192us)

Figure 12: Protocol data unit in the IEEE 802.11b.

To avoid the hidden-node collisions, the hidden nodes should not send a packet during the time (t_{fk}) where the t_{fk} is the time that the sender sends $k-th$ fragmented packet successfully. Then, the time t_{fk} can be represented as

$$t_{fk} = 2(T_{PLCP} + \sigma) + \frac{H_{mac} + F}{Data\ rate} + \frac{Ack\,Frame}{Ack\,Rate} + (2k-1)SIFS, \tag{3}$$

where T_{PLCP} is transmission time of PLCP preambles and headers, H_{mac} is MAC header, and σ is propagation time. To get the probability that the hidden nodes do not send a packet during the ongoing transmission time, where K is the number of fragmented packets, time (t_{fk}) need to be represented as the number of back-off slots (α_k) in Figure 13. Therefore, α_k can be expressed as

$$\alpha_k = \left\lceil \frac{t_{fk}}{slot\ time} \right\rceil , \tag{4}$$

where α_k is an integer. Note that the transmission probability of contending nodes ($\tau_{C_{ni}}$) is different from the transmission probability of hidden nodes ($\tau_{H_{ni}}$), since the number of transmission failure is different due to their different number of nodes. The probability that the hidden node (H_{ni}) do not send packets during the sender's transmission is $(1 - \tau_{H_{ni}})^{\alpha_k}$. If more fragmented packets are used, the number of back-off slots for the hidden collision α_k becomes bigger, and thus, this probability $(1 - \tau_{H_{ni}})^{\alpha_k}$ approaches close to zero. Hence, each individual fragmented packet's collision probability against hidden nodes could be reduced by using small fragmented size (Figure 13).

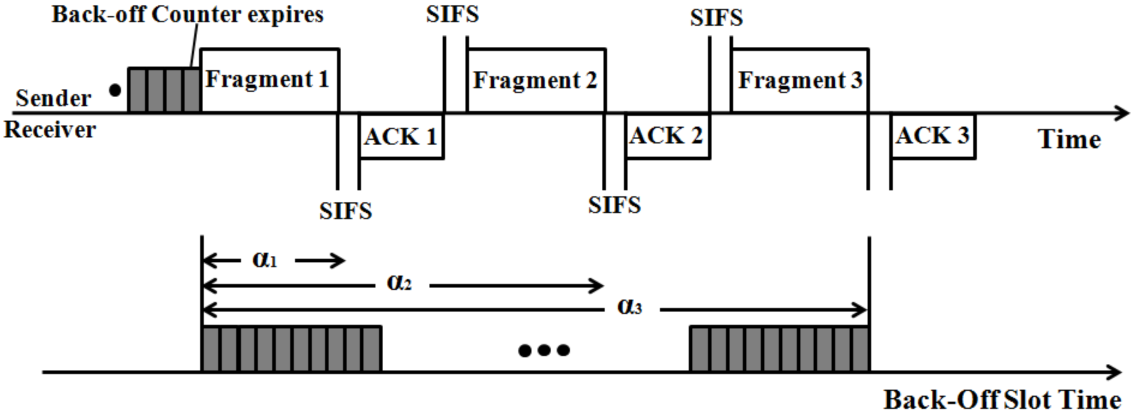


Figure 13: Vulnerable periods by number of back-off slots.

Lastly, even though the senders do not suffer collisions resulting from either contending nodes or hidden nodes, unsuccessful transmission still could be occurred in the bad BER channels because of the interference and noise. The probability that each fragmented packet does not have packet errors is $(1 - BER)^F$, (note that F is the length of a fragment) and the probability that the entire fragmented packets do not have any packet errors can be expressed as $(1 - BER)^{kF}$. Consequently, by incorporating all these three parameters, the probability of unsuccessful transmission for sender i (P_{total_i}) can be represented as

$$P_{total_i} = 1 - \prod_{P \in \beta i}(1 - \tau_P) \prod_{P \in \gamma i}(1 - \tau_P)^{\alpha_k}(1 - BER)^{kF}. \tag{5}$$

Considering Markov-chain regularity, we can get the simplified equation for $b_{0,0}$ in [2] as

$$b_{0,0} = \begin{cases} \frac{2(1-2P)(1-P)}{W(1-(2P)^{m+1})(1-P)+(1-2P)(1-P^{m+1})} & m \leq m^{'} \\ \\ \frac{2(1-2P)(1-P)}{W(1-(2P)^{m+1})(1-P)+(1-2P)(1-P^{m+1})+W2^{m^{'}}P^{m^{'}+1}(1-2P)(1-P^{m-m^{'}})} & m > m^{'} \end{cases}, \tag{6}$$

where m is maximum retry count limit, and $m^{'}$is 5. And we adopted the equation of τ in [2] that can be represented as

$$\tau = \sum_{i=0}^{m} b_{i,0} = \frac{1 - P^{m+1}}{1 - P} b_{0,0}. \tag{7}$$

With the Equation 5, 6, and 7, we can get the value of τ_i and $P_{total\,i}$ for all senders (from 1 to N) using numerical analysis.

3.2.3 Throughput Analysis

To derive the throughput equation for individual node, the probability that at least one node transmits a packet in a given back-off slot time is needed. Let P_{tr} be the probability that transmission occurs among contending nodes in a given slot time. The probability that Sender i does not transmit a packet in a given slot time is $(1 - \tau_i)$. Hence, the P_{tr} after considering all N nodes can be written as

$$P_{tr} = 1 - \prod_{i=1}^{N}(1 - \tau_i). \tag{8}$$

Denote P_{sk} be the probability that $k-th$ fragmented packet is successfully transmitted given the probability P_{tr}, then, we get followings:

$$P_{sk} = \frac{\sum_{i=1}^{N} \tau_i \prod_{P \in \beta i}(1 - \tau_P) \prod_{P \in \gamma i}(1 - \tau_P)^{\alpha_k}(1 - BER)^{kF}}{P_{tr}}, \tag{9}$$

where βi is a contending node set, γi is the hidden node set in perspective of Sender i. If fragmented packet transmission failed, the sender does not transmit the next fragmented packet by the standard. Thus, another probability is needed, which is the probability that $k - th$ fragmented packet is successfully transmitted, and the next $(k + 1) - th$ fragmented packet is failed. There can be two reasons that $(k + 1) - th$ fragmented packet is failed except for the first transmission time slot. The first reason is due to the collisions by hidden nodes, and the second reason is owing to the random-packet errors. Then, the probability that $k - th$ fragmented packet is successfully transmitted is

$$P_{s(k+1)} = \sum_{i=1}^{N} \tau_i \prod_{P \in \beta i} (1 - \tau_P) \prod_{P \in \gamma i} (1 - \tau_P)^{\alpha_k} (1 - BER)^{kF}. \tag{10}$$

Hence, the probability that $(k + 1) - th$ fragmented packet is unsuccessful ($P_{us(k+1)}$) can be written as

$$P_{us(k+1)} = (1 - \prod_{P \in \gamma i} (1 - \tau_P)^{(\alpha_{k+1} - \alpha_k)} (1 - BER)^F). \tag{11}$$

By incorporating Equation 9 and Equation 11, the probability (P'_{sk}) that $k - th$ fragmented packet is successfully transmitted and $(k + 1) - th$ fragmented packet is failed, can be represented as Equation 12.

$$P'_{sk} = P_{sk} P_{us(k+1)}. \tag{12}$$

Note that P'_{S1} means a probability of the first fragmented packet transmission is successful, and the second fragmented packet transmission is unsuccessful. In addition, P'_{S0} represents the probability that no packet is delivered successfully. We denote T_s as the average time that the channel is busy during successful transmission, T_c as the average time that the channel is busy with unsuccessful transmission after the ACK timeout. T_{sk} is the average time that the channel is busy with successful transmission during the successful transmission of $k - th$ fragmented packet and the failure of $(k + 1) - th$ fragmented packet. In addition, we define T_{sc} is the additional detection time when next fragmented packet is unsuccessful, and T_{ck} is the detection time when $k - th$ fragmented packet is unsuccessful. Then, we can express as

$$\begin{aligned} T_{sc} &= 2(T_{PLCP} + SIFS + \sigma) + \frac{H_{mac} + F}{Data\,rate} + \frac{Ack}{Ack\,Rate} \\ T_{sk} &= DIFS + t_{fk} \\ T_{ck} &= T_{sk} - 2\sigma, \end{aligned} \tag{13}$$

where T_{PLCP} is the transmission time of PLCP preambles and headers, H_{mac} is MAC header, and σ is propagation time.

If the current fragmented packet is failed, MAC releases the channel and increases contention-window size to repeat the contending procedure. Thus, in each case, achieved throughput values are different. Let's define the throughput S_j, when the $j-th$ fragmented packet is transmitted successfully, and a $(j+1)-th$ fragmented packet is failed. Using the same definition of normalized throughput in [4], we have

$$S_j = \frac{E[Payload\,Information]}{E[Length\,of\,Time]} = \frac{P_{tr}P_{sj}E[L]}{(1-P_{tr})\sigma + P_{tr}P_{sj}(T_{sj}+T_c) + \sum_{i=0}^{j-1} P_{tr}P'_{S\,i}T_{c(i+1)}}. \quad (14)$$

Therefore, the total average throughput (S) can be represented as

$$S = \sum_{j=1}^{k} \frac{P'_{S\,j}}{\sum_{j=1}^{k} P'_{S\,j}} S_j. \quad (15)$$

Since the throughput equation (S) varies upon the different number of fragments (K), and different size of fragments (F), the optimal fragmentation size (F_{OPT}) can be founded where S reaches the maximum value. Eventually, the maximum throughput can be achievable based on the number of contending nodes, the number of hidden nodes, and random-bit errors without protocol modifications.

3.3 System Evaluation

3.3.1 Simulation Set Up

OPNET simulator [25] is used to validate our system model. All the parameters used in the analytical model and the OPNET simulation are summarized in Table 1. In the pipeline process model of the OPNET simulator [25], when nodes receive other packets while current packet is arriving, they immediately calculate the effective signal to noise ratio (SNR) of both previous packet and current arriving packet. Then, if the SNR value is lower than the packet-reception threshold, nodes discard the packets. In the simulation scenarios of this research, the hidden-node group and contending-node group are located at the same distance from a receiver in the opposite direction. Therefore, whenever the collisions occur by hidden nodes, nodes discard both the previous packet being received and the current arriving packet at the same time like the actual collision effect in the wireless network. The total number of nodes is 10, the random-bit error rates varies from 10^{-5} to 1.5×10^{-4}, the data rate is 11 $Mbps$ that uses CCK (complementary code keying), and the propagation delay is 1 μs.

Table 1: Simulation parameters.

Data frame retry limit	5	Modulation	CCK
Control frame retry limit	7	Propagation Delay	1 µs
Number of CN	10 to 6	Slot Time	20 µs
Number of HN	0 to 4	MAC header + FCS	28 Bytes
BER	10^{-5} to 1.5x 10^{-4}	PHY header	24 Bytes
IP header + UDP Header	28 Bytes	Packet Payload	1500 Bytes
Data Rate	11 Mbps	ACK Size	14 Bytes
ACK Rate	1 Mbps	$C_{WIN_{min}}$	31
DIFS	50 µs	$C_{WIN_{max}}$	1023
SIFS	10 µs	Simulation Time	180 seconds

3.3.2 Simulation Results

To separate the effect of fragmentation technique on BERs from effect on hidden-node collisions, analysis of fragmentation under different BERs must be validated separately in this simulation, even though many previous works with fragmentation are done such as in [12]. Hence, in the first scenario, one receiver is located with 10 senders at the same distance from the receiver. Therefore, the receiver maintains the same BER for all the packets coming from the senders in the first simulation. Each 10 contending node generates a 1500-byte packet to the receiver every 0.0001 seconds to saturate the 11 $Mbps$

channel. The fragmentation-packet size is changed with different BERs, e.g., 10^{-5}, 2.2×10^{-5}, 10^{-4}, and 1.5×10^{-4}. The throughput result of the receiver for fragmented-packet size is shown in Figure 14. The throughput, when BER is 10^{-5} that generally represents the normal channel condition, is decreasing when fragment packet sizes become small because of the fragmentation overheads (additional SIFS intervals and ACKs). However, under the bad channel conditions such as 10^{-4} and 1.5×10^{-4}, the throughput starts to improve. Moreover, each optimal fragmented packet size changes, which are 750 bytes (two 750-byte fragments) when BER is 10^{-4}, and 500 bytes (three 500-byte fragments) when BER is 1.5×10^{-4}. Although the packet-error rate (PER) becomes smaller as the fragmented packets are smaller, the fragmentation overheads sacrifice this benefit. Hence, small fragments do not always guarantee high network throughput.

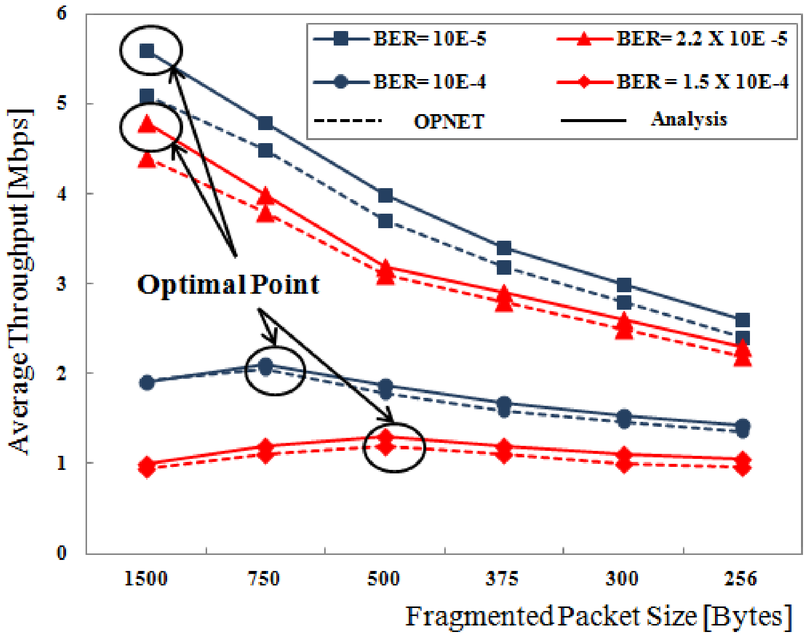


Figure 14: The simulation results of conventional fragmentation effects on BER.

In the second scenario, to compare the effects of hidden terminals equally, the number of hidden nodes changes from 0 to 4, while the number of contending nodes varies from 10 to 6. Therefore, the total number of nodes remains same as 10, excluding the receiver. The BERs in the second scenario are 10^{-4} and 10^{-5}, which generally represent bad channel condition and normal channel condition, respectively. We compare the result using optimal packet fragmentation with the result using RTS/CTS exchange mechanism, because other mechanisms require the protocol modification, which is hard to implement in the OPNET simulator. The performance results with respect to hidden-node collisions are presented in Figure 15, 16, and 17. In Figure 15, when just one hidden node is added to the network, the throughput can be increased by 16% with 750-byte fragment size compared to the RTS/CTS exchanges under 10^{-5} BER. When the BER becomes worse to the 10^{-4}, the throughput with 500-byte fragment size is better performed by 27% rather than RTS/CTS exchanges. As the number of hidden nodes increased up to 3, and thus, frequent hidden-node collisions occur, the throughput with fragmentation is still better by 25% more than RTS/CTS exchanges as shown in Figure 17. This result indicates that the optimal fragmentation can significantly reduce the retransmissions by both random-bit errors and hidden-node collisions, even though it cannot perfectly escape the hidden-node collisions. The optimal fragmented packet size also varies to compensate the collisions from the hidden nodes, e.g., 750 bytes when HN is 1, and 500 bytes when HN is 3 under 10^{-5} BER. Although the total hidden-node collision back-off slot time (α_k) is increased because of the fragmentation overhead (Figure 13), each back-off slot of fragmented hidden node such as α_1 is reduced by the fact that smaller fragments give more chances to escape from the collisions caused by fragments of the hidden nodes. Especially, when the number of hidden node is three and the number of contending node is seven under 10^{-4} BER (Figure 17), the throughput continues to increase until the fragment is 375 bytes. However, for the smaller fragments below the optimal fragment, the overhead of fragmentation sacrifices the benefit of using smaller fragments, which eventually reduces the network throughput.

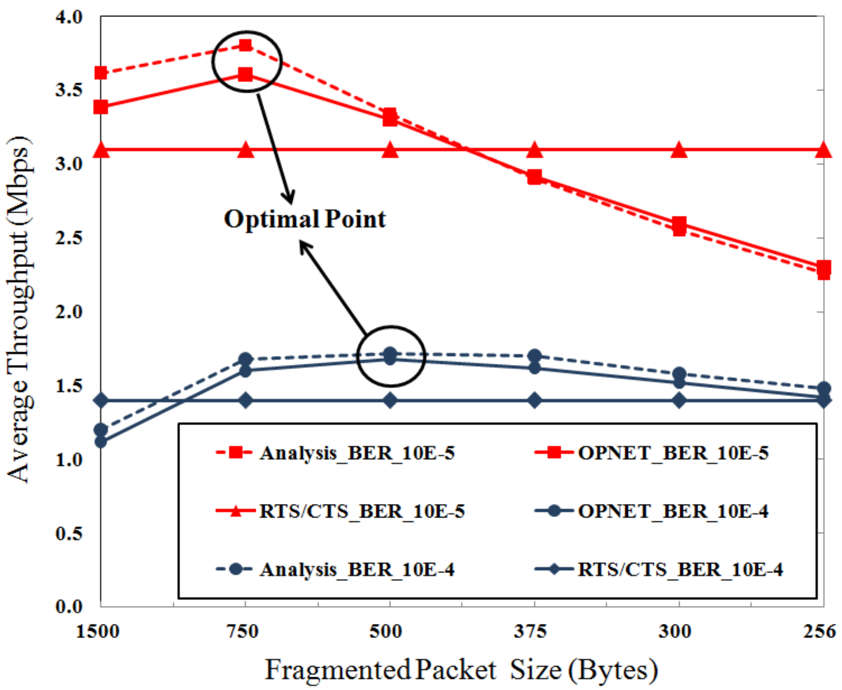


Figure 15: The simulation results when 9 contending nodes and 1 hidden node.

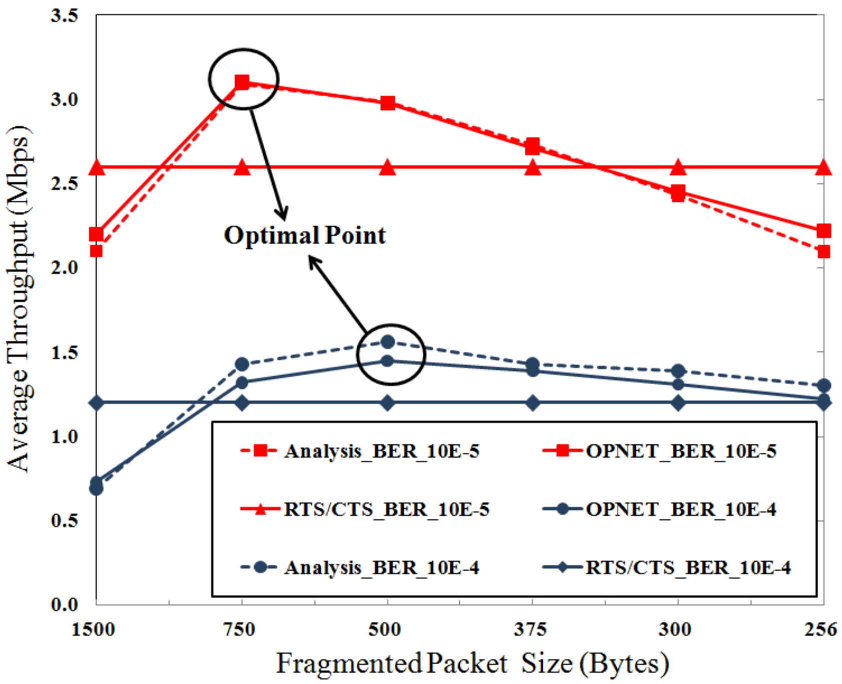


Figure 16: The simulation results when 8 contending nodes and 2 hidden nodes.

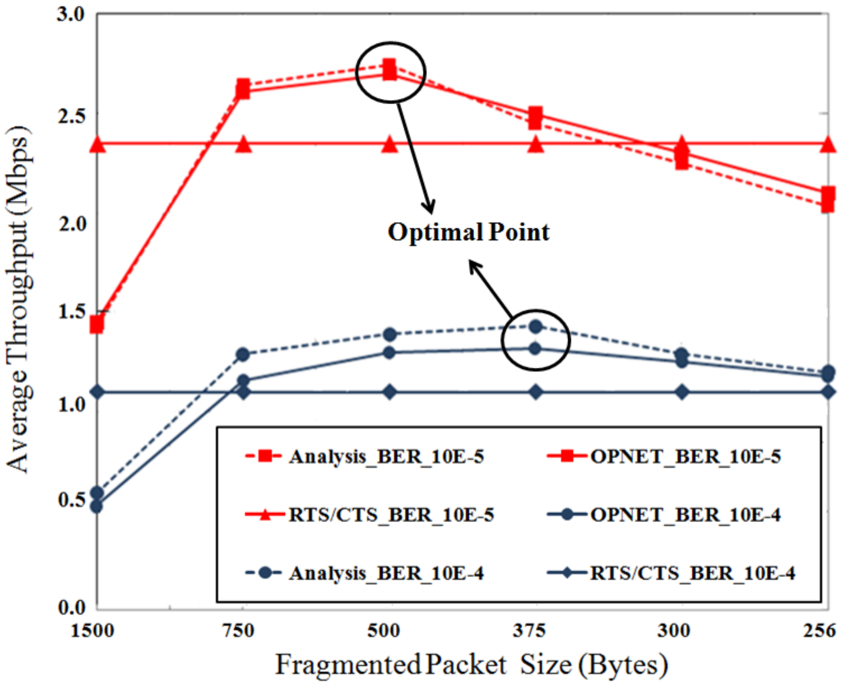


Figure 17: The simulation results when 7 contending nodes and 3 hidden nodes.

The comparison between the throughput with optimal fragmentation and RTS/CTS exchanges under various parameters is summarized in Figure 18. The optimal fragmentation is generally better performed than RTS/CTS exchange in our simulations which are very similar to real MANETs environments. Nevertheless, if the number of hidden node is dominant factor in the network, the RTS/CTS exchange may be more desirable. However, the condition that there are more than four hidden nodes in the network is rarely happened. Nevertheless, RTS/CTS exchange has no effect to the random-bit errors when the interference is severe. In addition, the control signals (RTS/CTS signals) also can be lost when the channel is noisy (high BER). The limitation of this research lies on how senders know if hidden nodes exist in our networks. However, fragmentation method proposed in this research can be easily merged into the intelligent algorithm described in [12].

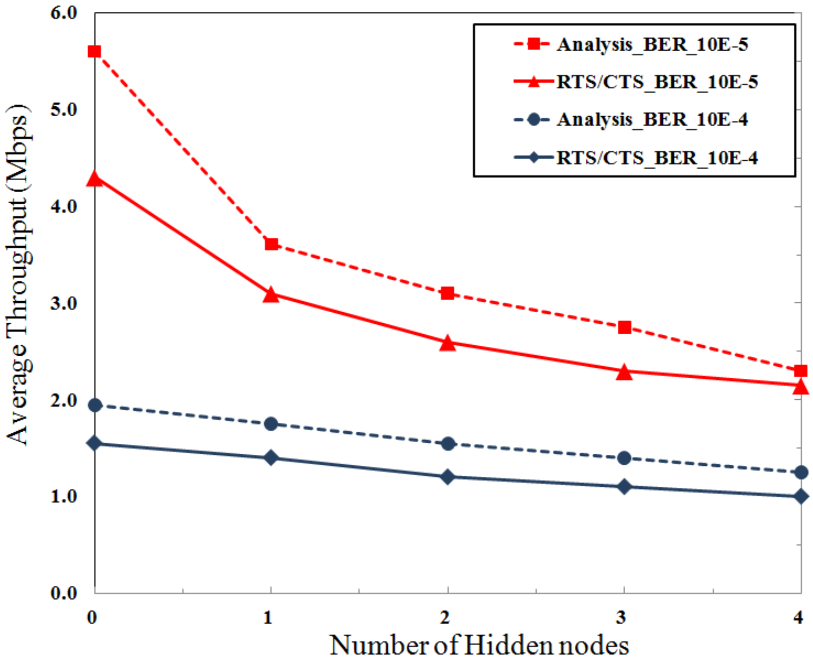


Figure 18: Overall comparison of throughput with RTS/CTS.

3.4 Experimental Evaluation

Although the optimal fragmentation is evaluated in various simulation environments, the deployment issue should be considered in the real out-door environment that is dynamic and challenging. While most of efforts to solve a hidden-node problem have been focused on the theoretical analysis, very little efforts were given to the verification of proposed models through real-world experiments. Therefore, the experimental result will be analyzed in this subsection.

3.4.1 Experimental Set up

General parameters in our experiments are listed in Table 2. The payload size is 1500 byte, data type is UDP (User Datagram Protocol), and 11 Mbps data rate is used. To validate our analysis, six Orinoco Proxim Gold LAN cards [26], and external antennas are used for 802.11b ad-hoc mode and six laptops (Lenova R400) are used for mobile stations (Figure 20). Ubuntu version 6.1 and mad WiFi driver for configuring parameters (Table 2) to achieve system stability are installed in each station. The outdoor environments depicted in Figure 19 have 8 meters by 20 meters area surrounded by several buildings. Therefore, we believe that several interferences and multi-path fading exist as well. The SINR values and throughput values (sample per every 10 ms) are displayed in the station monitor. The throughput result and the corresponding SINR values are averaged using more than 1000 samples in our results.

Table 2: Experiment parameters

Experiment Area	8m x 20m
Tx Power	1 dBm ~5 dBm
Channels	Channel 3(2.422GHz) Channel 8(2.447GHz)
Average Noise Level	-95 dBm
Data Rate	11 Mbps
Data Type	UDP
SNR Range	10 dB to 16 dB
Modulation	CCK (complementary code keying)
Packet Payload	1500 Bytes

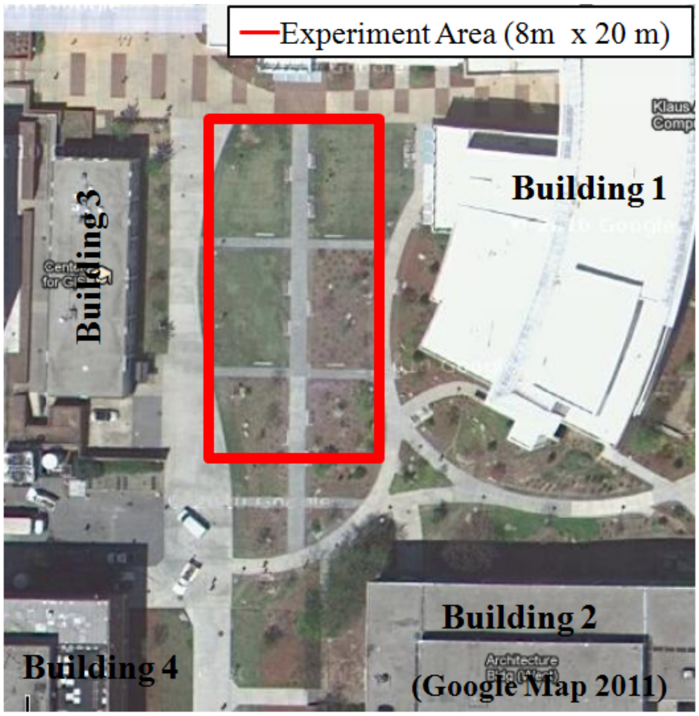


Figure 19: Experimental Area (Klaus Bd., Georgia Tech, GA 30332).

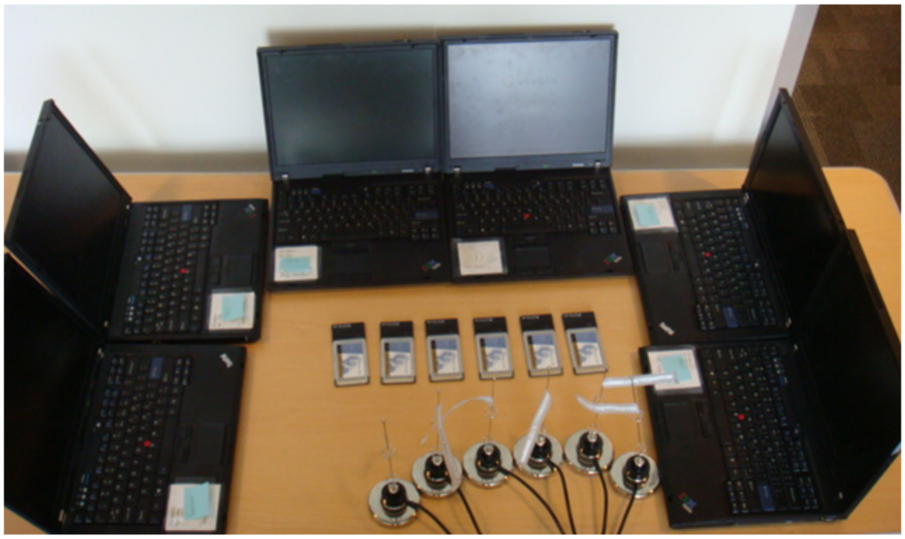


Figure 20: Experiment devices (Lenova R400, Orinoco Proxim Gold LAN cards, and external antennas).

Figure 21 illustrates Scenario one to compare our suggested fragmentation with RTS/CTS exchanges in real time. To compare the average throughput of each technique precisely, two senders, two receivers, and two hidden nodes are located in the same geographical locations (see Figure 21). The fragmentation group uses the Channel 3 and the RTS/CTS group use Channel 8, so that each group does not interfere to each other. During the experiments, we figured it out that among the adjacent channels such as Channel 3, and Channel 4, each station in different channel can actually communicate and sense to each other, hence, exact comparison could be impossible. This is because of the hardware characteristic, even though they are not in the same channel, they automatically change their channels so that they can communicate to each other.

Figure 22 depicts Scenario two, when 2 groups exist and they are competing to each other. In each group, there are two nodes competing for the medium access, at the same time, they are hidden to each other. While Scenario one gives us the impact of hidden-node collision, Scenario two provides more realistic results than Scenario one, because the hidden nodes have generally contending nodes in the neighbors.

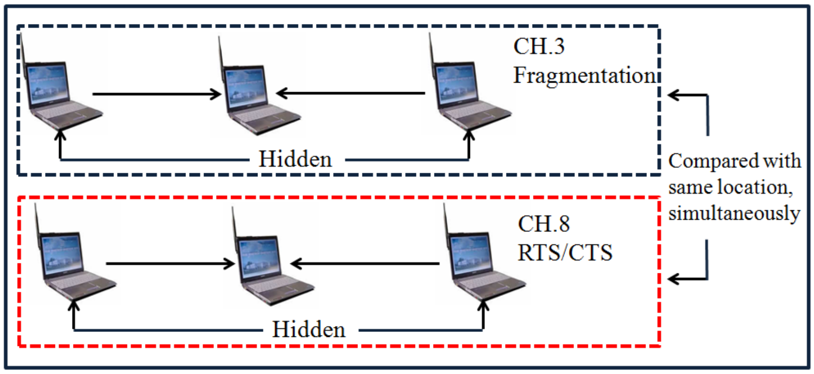


Figure 21: Scenario One configuration.

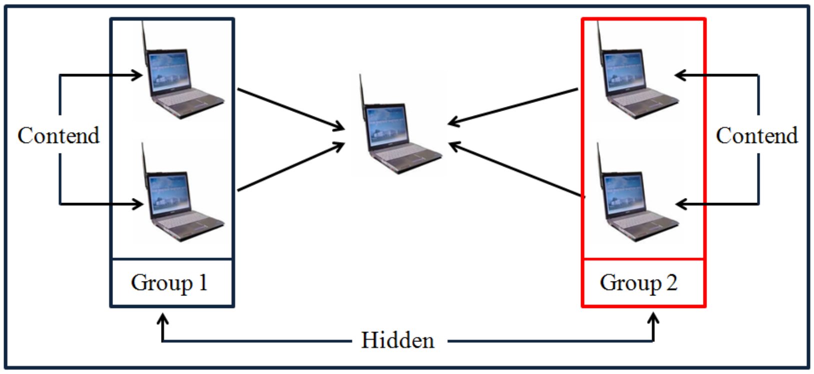


Figure 22: Scenario Two configuration.

On the other hand, since the noise level and the received signal strength in the receiver (these are known parameters from the wireless LAN cards) keep slightly changing with the same geographical locations during our experiments, the throughput and SNR values at the receivers are recorded every 10 ms. Moreover, because the channel conditions vary under different weather conditions, the same experiments are performed with same parameters in the morning and at night to obtain the average of six results in total.

To characterize our wireless environments for the experiments, the average SNR (Signal to Noise Ratio) value is measured in every 0.5 meter by transmitting 32-byte ping packets for 300 seconds with 1-dBm transmission power as shown in Figure 23. In addition, during the experiments, transmission powers are required to be regulated to generate target SNR values and target number of hidden nodes. If the SNR value in the receiver falls below average of 5 dB, receivers could not receive any packets from the sender due to low SNR values, even though they can decode packets theoretically. Between 5 dB and 10 dB SNR values, numerous packets are dropped, hence, the communication is unstable for the experimental measurements. Therefore, the SNR ranges are targeted from 10 dB to 15 dB in order to get accurate throughput results.

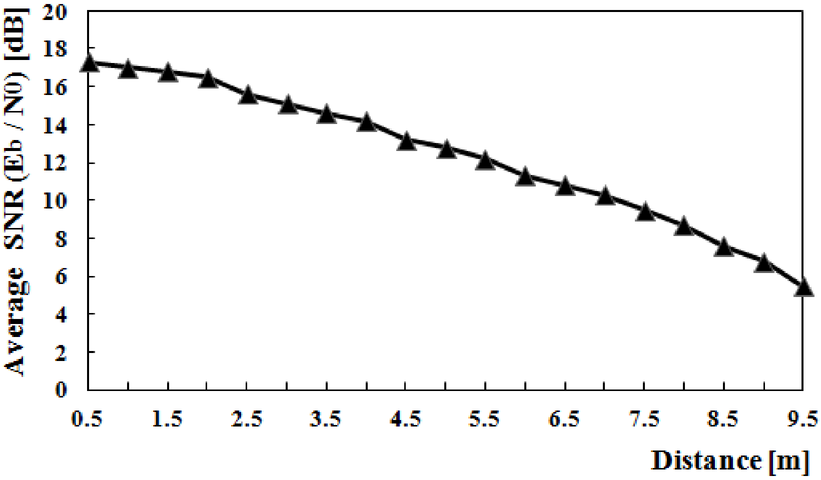


Figure 23: Average SNR values by distances in one-hop transmission.

For investigating the fading characteristics in wireless channels, we also measured average throughput with respect to the average SNR values. Using an OPNET simulator [25], these values are used to find proper approximated Rician factor K. The average SNR values and corresponding BERs are compared with theoretical IEEE 802.11b 11Mbps (data rate) complementary code keying (CCK) Rician fading model curves [27]. As shown in Figure 24, the environments roughly follow the trend with minor deviations at K Factor 10, which is a typical value for suburban areas.

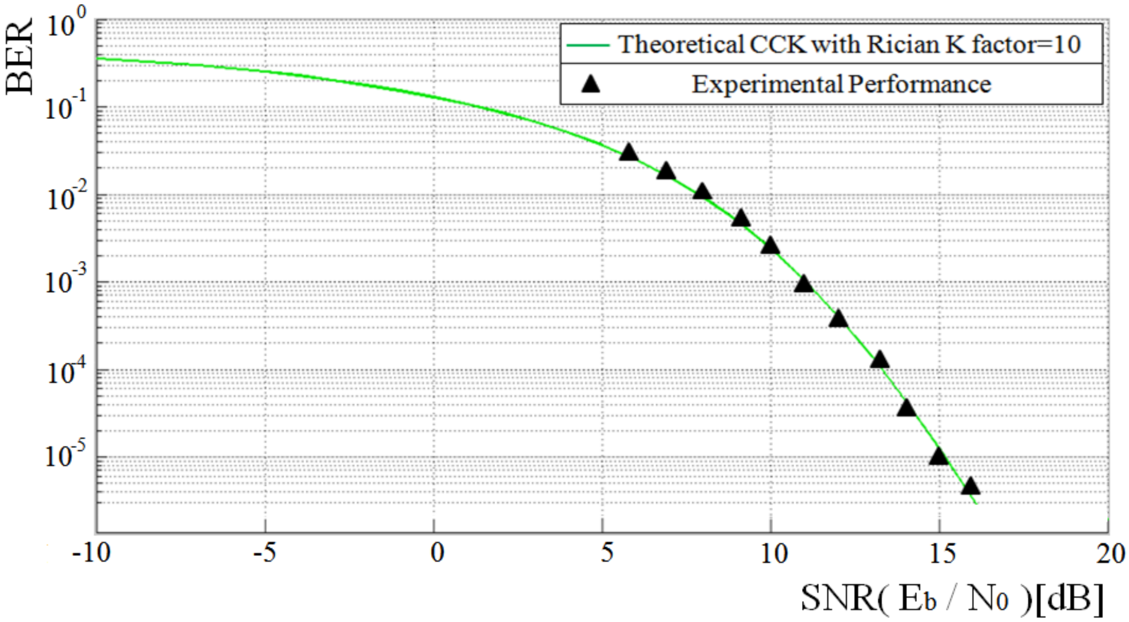


Figure 24: Rician channel fading curves and experimental BERs.

3.4.2 Experimental Results

The optimal fragmentation sizes and the corresponding SNR ranges in our experiments are suggested in Table 3 based on our theoretical analysis [24], channel information, and the scenarios. Since the payload size is 1500 byte, 750-byte fragment size means two fragmented packets, 500-byte fragment size means three fragmented packets. However, because the minimum fragmentation size by the IEEE standard is 256 bytes, we used 256 bytes rather than 250 bytes in our experiments. Although the number of hidden node is precalculated in advance, we used the channel estimation algorithm (see [12]) that gives accurate SNR-estimation values, and thus, each station automatically changes the optimal fragmentation size based on the Table 3 in real time.

Table 3: Suggested fragmentation size.

Scenario	SNR [dB]	Fragmentation Size [Bytes]
1	14.7 dB ≤SNR	750
1	13.3 dB ≤ SNR < 14.7 dB	500
1	12.4 dB ≤ SNR < 13.3 dB	375
1	11.7 dB ≤ SNR < 12.4 dB	300
1	SNR < 11.7 dB	256
2	15.2 dB ≤ SNR	750
2	14.1 dB ≤ SNR < 15.2 dB	500
2	13.2 dB ≤ SNR < 14.1 dB	375
2	12.4 dB ≤ SNR < 13.2 dB	300
2	SNR < 12.4 dB	256

In the first scenario, the distances from the senders to the receiver are regulated depending on the target SNR values. This SNR range is from 10 dB to 15 dB, and their corresponding bit-error rates are from 5× 10^{-2} to 2× 10^{-5} (Figure 24). The average throughput values of the first scenario are shown in Figure 25 for the proposed optimal fragments and the RTS/CTS mechanism. When the packet-error rate (PER) is not high , and thus, it is not the major reason for the transmission failures (i.e., average SNR is 15.3 dB), the hidden-node collision is a dominant factor in the network throughput. In this particular channel with 15.3 dB SNR, the proposed optimal fragments improve throughput by 68% more than the RTS/CTS exchange. This result indicates that exchanging RTS/CTS signals sacrifices more bandwidth than transmitting two 750-byte fragments. Consequently, by choosing optimal fragments, the network throughput can be significantly increased by reducing the hidden node collision probabilities and overheads of RTS/CTS control signal exchanges.

When the channel condition is poor (i.e., average SNR is 10.4 dB) in Figure 25, the throughput of fragmentation is 180% more than the throughput of RTS/CTS. In this case, the transmission failures occur frequently by both high BER and collisions because of hidden nodes. Therefore, the saturated contention-window size eventually becomes large by the unsuccessful transmissions. Thus, the probability of hidden-node transmission during the vulnerable periods becomes small. These small transmission probabilities of hidden nodes also make the hidden-node collision probabilities to be small because of inflated contention windows at hidden nodes. Eventually, the transmission failures by random-bit errors dominate the entire transmission. While fragmentation effectively escapes from the collisions imposed by high BERs, the RTS/CTS has no effects over the BERs. Therefore, using fragmentation technique is more desirable than using RTS/CTS exchange in this case.

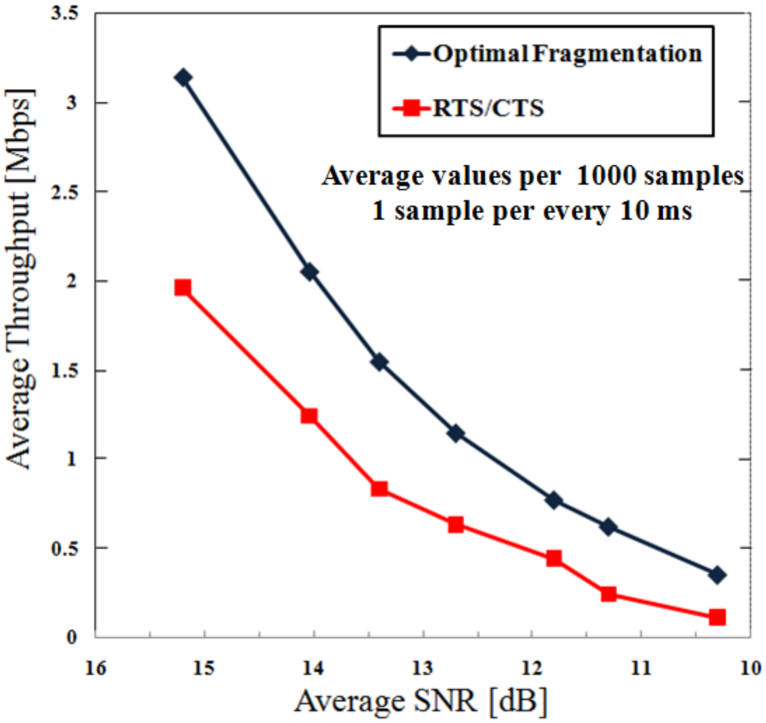


Figure 25: Average experimental-throughput comparison in Scenario one.

The average throughput values are shown in Figure 26, when two groups are hidden to each other, and each group has one contending nodes except for the sender (Scenario two). Each group starts transmissions to the receiver located between two groups. The results for fragmentation are compared with RTS/CTS.

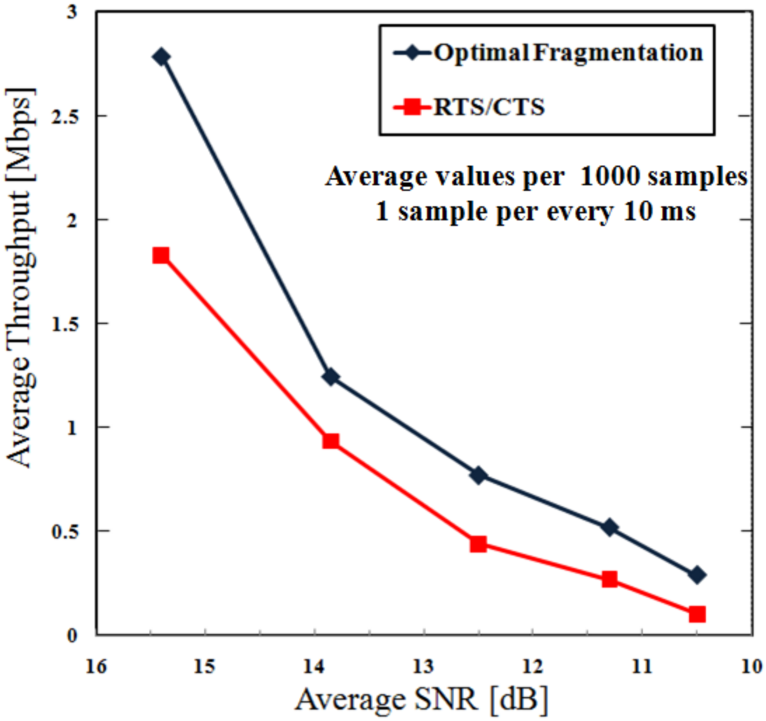


Figure 26: Average experimental-throughput comparison in Scenario two.

When the average SNR is 15.4 dB, the average throughput values are lower than the Scenario one, as a result of the competitions among the contending nodes (see Figure 22). However, the throughput of optimal fragmentation is still 45% better than the throughput of RTS/CTS exchanges. In the perspective of sender in Group one, it has two hidden nodes that competes to each other. After competing to the channel, only one hidden node starts to transmission during the transmission time of sender. Therefore, the hidden-node collision probability is higher than the Scenario one. RTS/CTS exchanges can remove those hidden-node collisions, nevertheless, optimal fragmentation also reduce the hidden-node collision probability as well. Therefore, our experimental results imply that fragmentation is more efficient for hidden-node problems than RTS/CTS exchange in this scenario. When the average SNR becomes 10.2 dB, our optimal fragmentation has positive effects on both packet errors and hidden-node collisions with smaller overheads than RTS/CTS exchange. After all, the entire network throughput is better than RTS/CTS exchanges by 150%. Since the contention-window size also becomes larger than 15 dB channels, the hidden-node collision probability is also reduced in 10.2 dB SNR channel. Throughout our experiments, we showed that an optimal fragmentation increase network throughput without any deployment issues in noisy channel conditions.

3.5 Contribution and Limitation

Throughout our analysis, extensive simulations, and experiments in this chapter, we showed that an optimal fragmentation could increase the network throughput in hostile channel conditions, i.e., low SNR and collisions from hidden nodes. The RTS/CTS exchange is powerful in reducing the collisions from the hidden nodes. Nevertheless, RTS/CTS exchange has no effect in alleviating random-bit errors, when the mobile communication channels are in poor conditions. As shown from the simulation and experiment results, the optimal fragments are more effective than RTS/CTS exchange in dealing with both BERs and collisions from the hidden terminals. Since the other works on the hidden-node problems require the protocol modifications, we cannot compare the other works with our results through experiments. Besides, we also observed that the control frames (RTS/CTS) are frequently lost due to the noisy environments during the experiments, while the simulation does not include this effect, thus, the improvement of the throughput in our experiment is much higher than in the simulation results. Therefore, the algorithms using control frames to solve the hidden-node problem is not efficient in the noisy channel.

One challenging problem in solving the hidden-node problem through our optimal fragmentation is that how we could know how many hidden terminals exist in the network and SNR values to incorporate the analytical results. Since this research more focuses on the accurate effects of both various BERs and different number of hidden nodes on the network throughput through real experiments than the fully automated implementation of our scheme, we calculate the optimal packet size in advance during the experiments. However, SNR values can be estimated accurately from [12], and the total number of nodes can be obtained by observing different MAC addresses. To get the number of hidden nodes, each sender could exchange the number of neighbor lists in the routing tables and could hear the acknowledgment packets from the receiver to other hidden nodes that are out of carrier sensing range of the sender. However, the detailed procedures for estimating the number of hidden nodes remain as a future work. Fortunately, optimal fragment lengths are not very sensitive to the number of hidden nodes and the exact SNR values in our analysis and experiments (see Table 3), fragmentation method proposed in this research is more robust than other research that requires the exact number of hidden nodes.

The contribution of this research is to investigate the impact of both hidden nodes and random-bit errors (BERs) with respect to the fragment lengths through the analysis, simulation, and real-world experiments in noisy mobile ad-hoc networks (MANETs), while the conventional research on the hidden-node problem has concentrated on the problem itself by suggesting alternative algorithms including evaluation of RTS/CTS handshaking in ideal channel conditions (simulations). Unlike most of the existing fragmentation methods, which mainly focused on the random-bit errors for the channel conditions, this study incorporates hidden terminals and fragment length as well as BERs. Throughout real-world experiments under different weather condition, fading characteristic, and distances between nodes, we found that the hostile environment (low SNR and collisions from hidden nodes) deteriorates the network performance significantly. Moreover, as we observed in our experiment and other researchers indicated, the control frame exchanges including RTS/CTS signals not only waste channel resources, but also are frequently lost due to the high BERs and collisions especially in noisy environments. As a result, optimal fragmentation could enhance network throughput more than RTS/CTS exchange, when the channels suffer from hidden nodes and random-bit errors simultaneously. Furthermore, this method can be used in real-time by incorporating a dynamic intelligent optimization protocol for channel estimation such as [12] that does not require IEEE 802.11 protocol modifications.

This work will provide a valuable real-world research results for the research communities to solve the hidden-node problem especially in noisy MANETs. Consequently, the novelty of this work lies on that the enhanced throughput can be achievable and implemented in real devices without deployment issues to solve both the hidden-node problem and random-bit errors simultaneously in noisy MANETs.

As an extension work, the optimal packet fragmentation need to be validated under vehicular ad-hoc networks (VANETs) that is a subset of mobile ad-hoc network. Since the protocol of VANETs (IEEE 802.11p) has some different characteristics from the general IEEE 802.11 MAC protocol, the details of analysis and validation will be discussed in the following chapter.

CHAPTER 4

FRAGMENTATION IN VEHICULAR AD-HOC NETWORKS

This chapter introduces the overview of the vehicular ad-hoc networks (VANETs) as a subset of mobile ad-hoc networks. As a standard for the vehicular ad-hoc networks, the IEEE 802.11p Standard was finalized in 2010. The IEEE 802.11p has some distinctive features from the conventional mobile ad-hoc networks such as dedicated short range communications (DSRC) and wireless access in the vehicular environment (WAVE) protocol. Therefore, our fragmentation technique should incorporate these effects on fragments size. In the following section, we will focus on the characteristic of communication in MAC layer with main features of VANETs. In the second section, we will formulate new equations and evaluate the optimal packet-fragmentation technique in VANETs. We will validate the simulation results compared to RTS/CTS handshaking mechanism in Section 4.3. In the last section, we will discuss about the results and limitations.

4.1 Introduction of Vehicular ad-hoc Networks

The momentum of research interest on vehicular ad-hoc networks (VANETs) has been accelerated, since the IEEE 802.11p Standard was finalized in 2010 to meet the demand for high mobile and dynamic operating environments [28]. Due to its high-mobile characteristic and dynamic operating environments, a reliable technology is required for the vehicle-to-vehicle communication (V2V) and vehicle-to-infra-structure (V2I) communication. To support intelligent transportation systems (ITS) applications for inter-vehicle communications such as safety-warning messages and traffic-information exchanges between high-speed vehicles, the IEEE 802.11p protocol for VANETs is based on dedicated short range communications (DSRC) at 5.9 GHz band. In DSRC, seven channels are allocated with each 10 MHz bandwidth, which consist of one control channel (CCH), four service channels (SCHs), and two other channels for high power and accident avoidance, as shown in Figure 27. The control channel (CCH) is designed for vehicle safety and control purposes, which are critical applications in VANETs. Each vehicle keeps alternating between a control channel (CCH) and one of the service channels (SCHs) during their CCH and SCHs intervals to check the control and safety messages periodically [29].

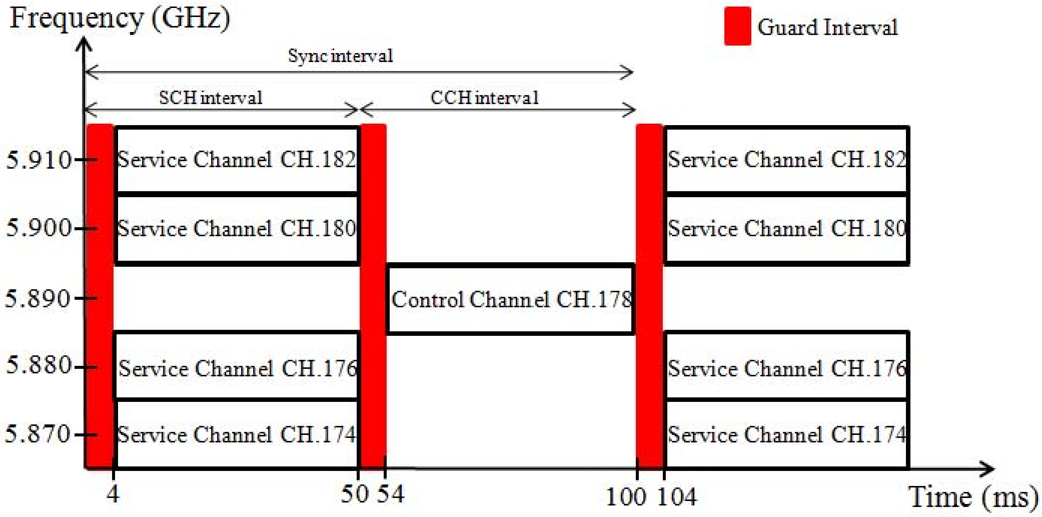


Figure 27: Multi-channel illustration in VANETs.

Besides, wireless access in the vehicular environment (WAVE) protocol provides priority access-category service based on the message types, which is equivalent to the IEEE 802.11e enhanced distributed channel access (EDCA) quality of service extension (QoS). In EDCA, four different access category (AC) is defined based the data type and priority. For example, AC3 has highest priority, while AC0 has no priority such as general data as described in Table 4. The real-time messages and safety messages, which belong to access category 3 (AC3), have shorter contention-window size and shorter inter-frame spaces (IFSs) than general data (AC0). Therefore, they could access the channel faster than general messages (Table 4). As summarized in Table 4, each access category has different maximum contention-window size. This limited maximum contention-window size allows each station, which has higher priority data, to have priority over general packets, even though this station increases its contention-window size by the collisions based on exponential back-off of the contention window.

Figure 28 gives an overview of EDCA architecture in VANETs. With four access categories that have different minimum and maximum contention-window sizes, each message competes for the internal contention procedure [30]. More specifically, every node inserts a data packet into one of four different queues depending on the data type (Figure 28) corresponding to four access categories (AC). Then, each queue keeps counting down its contention slots until it reaches zero, if the channel is idle. When contention slots expire in each queue, each node starts to access the channel.

There could be a virtual collision between different access categories within a single node. In this internal collision situation, the data that have lower access category must defer their channel access, and increase their contention-window size as double, while the data that have higher priority start its transmission, immediately.

AC	Data Type	CWmin	CWmax	AIFSN	AIFSN (slot = 13μs)
0	Background	15	1023	9	117 μs
1	Best Effort	7	15	6	78 μs
2	Voice	3	7	3	39 μs
3	Video	3	7	2	26 μs

Table 4: Congestion-window size and AIFSN based on access category.

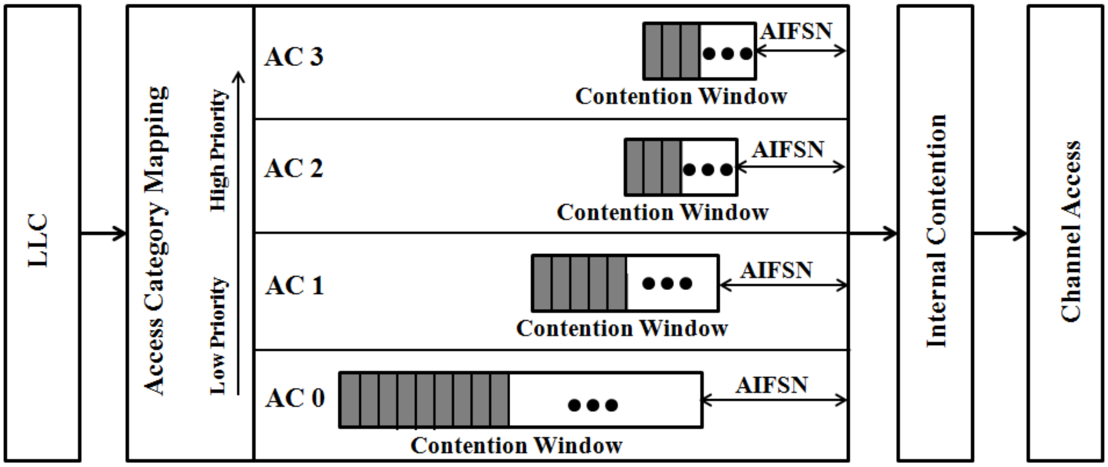


Figure 28: Internal-contention procedures in WAVE protocol

4.2 New Analysis of Packet Fragmentation

In our analysis in the previous chapter, the current contention-window size is critical to determine the transmission probability (τ) in a certain slot time, because nodes keep count down the current contention-window slot until it becomes zero, and start transmissions when channel is idle. In VANETs, four different access categories (AC) in WAVE protocol have different minimum and maximum contention-window sizes and arbitration inter frame sequence number (AIFSN) based on access categories as described in Table 4. This different contention-window size setting has a direct impact on the transmission probability in the network. Therefore, the WAVE effect on the packet fragment size must be investigated in our system analysis.

Our new fragmentation analysis will be based on the well-investigated work of EDCA under saturation condition [31] so that we can incorporate the WAVE characteristics in VANETs. Nevertheless, the authors in [31] did not consider random-bit error effect by interferences, hidden-node collision, and packet fragmentation feature that is related to the probability of that a node increase the current contention-window size as double up to maximum contention-window size.

4.2.1 Assumptions

We assume that every node has all four different access categories data to transmit with same packet length. When all nodes generates different access categories data (random traffic case), they experience the internal-contention procedure. If all nodes generate only specific access category data (deterministic traffic case), they do not experience the internal contention procedure. We will consider both cases. The other assumptions in this section are similar as in Chapter 3: There are contending nodes (C_{ni}), and hidden nodes (H_{ni}), and their corresponding numbers are βi and γi in perspective of a Sender i (Tx_i), respectively. Therefore, every sender i (Tx_i) has the different number of contending (βi), and number of hidden nodes (γi) regarding on its corresponding destination (Rx_i), and the total number of senders is N. The set of senders can be expressed as $\{Tx_1, Tx_2, Tx_3 \ldots\ Tx_N\}$, the set of contending nodes for Sender i (Tx_i) can be represented as a set of $\beta i = \{C_{n1}, C_{n2}, C_{n3} \ldots\ C_{n\beta i}\}$, and a set of hidden nodes for Sender i (Tx_i) can be expressed as a set of $\gamma i = \{H_{n1}, H_{n2}, H_{n3} \ldots\ H_{n\gamma i}\}$. The Sender i (Tx_i) could be the hidden node of some senders, the contending node of other senders, since they are competing for the medium access in the network. The number of fragmented packet is K, and the number of back-off slots of K packets transmission time is α_k.

4.2.2 New Markov-chain Model

The IEEE 802.11e enhanced distributed channel access (EDCA) protocol has some different features from distributed coordination function (DCF) in the medium access control (MAC) layer: While the back-off counter range in DCF is from 0 to $W_i - 1$, it is from 1 to W_i in the IEEE 802.11e EDCA. In DCF, the probability that the back-off counter decrease is one as depicted in Figure 11. However, the back-off counter in EDCA decrease with probability one after the end of AIFS.

The highest priority is AC0 in [31], but in this analysis, AC3 is highest priority-access category as same as the WAVE priority in VANETs. To avoid the confusion of notations with [31], we used the same parameters, but we incorporate the random-bit errors and the hidden-node collisions. Let τ_j denote the transmission probability of AC_j where j=0,1,2,3. $PC_{total\,j}$ is the probability that access category j increases the current contention-window size as double up to its maximum contention-window size. PT_j is the probability that the back-off counter of access category j is decreased by one. M_j is the maximum number of that AC_j can double the contention-window size, and M_j+f_j is the frame retry limit where f is the difference between M and frame retry limit. $W_{0,j}$ is the minimum contention-window size of AC_j. The internal (virtual) collision probability is PI_j. Figure 29 shows our new Markov-chain model incorporating random-bit errors, hidden-node collisions, and packet fragmentation in VANETs. Since each access category has different maximum contention-window size, M_j, f_j, $PC_{total\,j}$ varies depending upon the j in Figure 29.

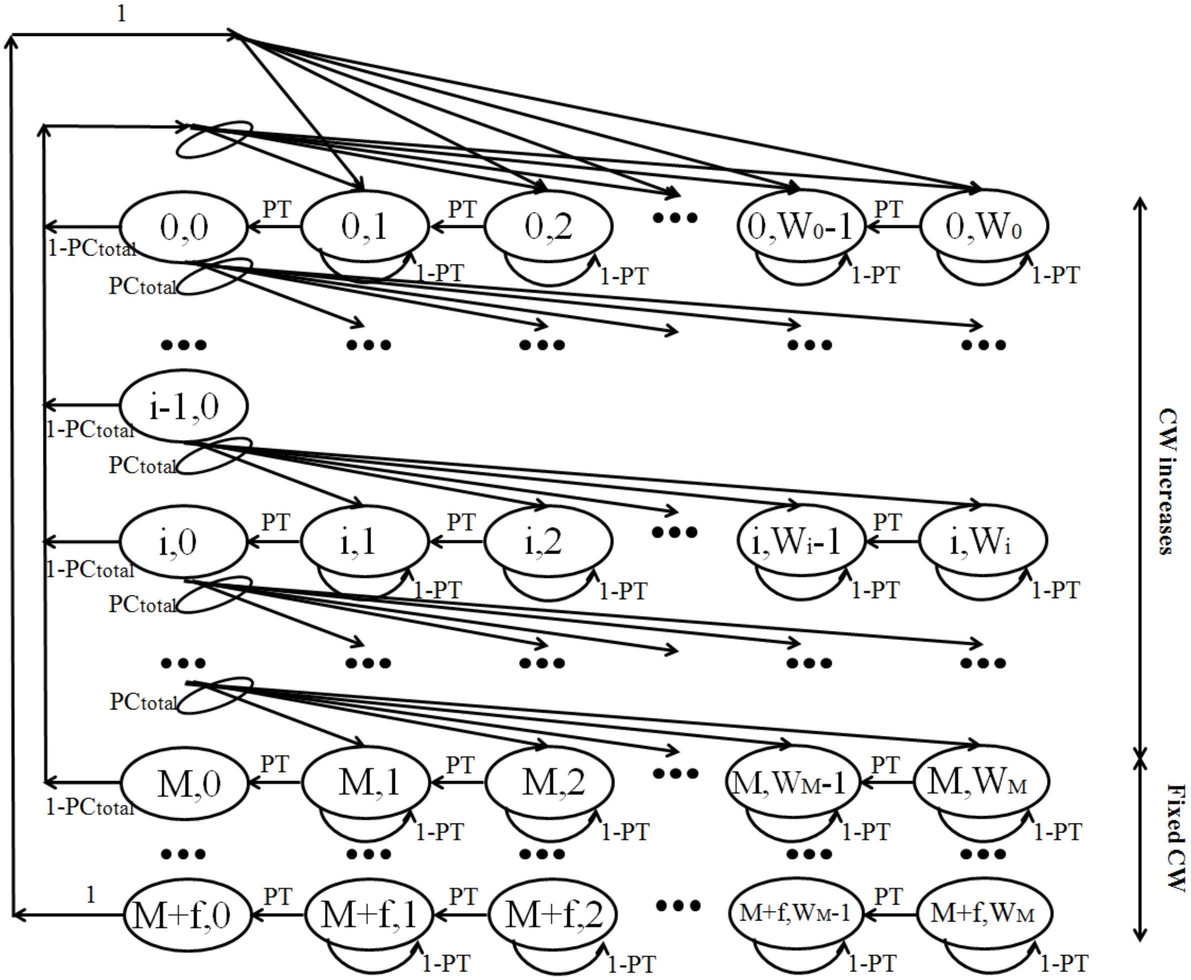


Figure 29: New Markov-chain model for single access category based on EDCA.

Note that the authors in [31] assumed that all nodes have four different access-categories data, and each access-category data competes for the internal contention. Our analysis also considered the case that each vehicle has one deterministic access-category data. Therefore, the internal (virtual) collision probability (PI_j) of the random traffic should be

$$\begin{aligned}
&PI_0 = 1 - (1-\tau_3)(1-\tau_2)(1-\tau_1) \\
&PI_1 = 1 - (1-\tau_3)(1-\tau_2) \\
&PI_2 = \tau_2 \\
&PI_3 = 0 \\
&\delta_0 = \tau_0(1-\tau_3)(1-\tau_2)(1-\tau_1) \\
&\delta_1 = \tau_1(1-\tau_3)(1-\tau_2) \\
&\delta_2 = \tau_2(1-\tau_3) \\
&\delta_3 = \tau_3 \qquad\qquad ,
\end{aligned} \tag{16}$$

where $\sigma_{total} = \sum_{j=0}^{3}\sigma_j$, σ_j denote the transmission probability of access category $j\,(AC_j)$ for the single station, and τ_j is transmission probability of AC_j in the internal contention in [31]. If each node has a deterministic access category, then, all the internal collision probability become zero, which means $PI_0 = PI_1 = PI_2 = PI_3 = 0$ and $\delta_j = \tau_j\, for\, every\, j.$ Let PO_{total} denotes the external collision probability by incorporating the effects of fragmentation and hidden-node collision. Then, PO_{total} can be written as

$$PO_{total} = 1 - \prod_{P\in\beta i}(1-\sigma_{total\,P})\prod_{Q\in\gamma i}(1-\sigma_{total\,Q})^{\alpha_k}(1-BER)^{Fragment\,size\,of\,AC}, \tag{17}$$

where βi is a set of contending node, and γi is a set of hidden nodes for sender. Therefore, after considering the internal collision, external collision, BERs, and hidden-node collision, the probability that access category j (AC_j) increase the current contention-window size ($PC_{total\,j}$) can be written as

$$PC_{total\,j} = PI_j + (1 - PI_j)PO_{total}. \tag{18}$$

The authors in [31] express the probability that the back-off counter decrease by one as PT_j, where j is the access category from 0 to 3. After considering the reverse order of the priority number, PT_j can be expressed as

$$PT_3 = \begin{cases} 0 & before\,AIFS_3 \\ 1 & after\,AIFS_3 \end{cases},$$

$$PT_2 = \begin{cases} 0 & before\,AIFS_2 \\ ((1-\tau_3)(1-\sigma_3)^{N-1})^{diff_2 - diff_3} & after\,AIFS_2 \end{cases},$$

$$PT_1 = \begin{cases} 0 & before\,AIFS_1 \\ ((1-\tau_3)(1-\sigma_3)^{N-1})^{diff_2 - diff_3}) & \\ \times(\prod_{j=2}^{3}(1-\tau_j)(1-\sigma_j)^{N-1})^{diff_1 - diff_2}) & after\,AIFS_1 \end{cases},$$

$$PT_0 = \begin{cases} 0 & before\,AIFS_0 \\ ((1-\tau_3)(1-\sigma_3)^{N-1})^{diff_2 - diff_3}) & \\ \times(\prod_{j=2}^{3}(1-\tau_j)(1-\sigma_j)^{N-1})^{diff_1 - diff_2}) & \\ \times(\prod_{j=1}^{3}(1-\tau_j)(1-\sigma_j)^{N-1})^{diff_0 - diff_1}) & after\,AIFS_0 \end{cases}, \tag{19}$$

where $diff_j \cong \frac{AIFS_j - DIFS}{a\ slot\ time}$.

Based on the above equations, we can get the transmission probability of AC_j (τ_j) using numerical analysis as follows [31].

$$\tau_j = \frac{2PT_j \times (1 - PC_{total\,j}^{M_j+f_j+1})}{(1+2PC_{total\,j})(1 - PC_{total\,j}^{M_j+f_j+1}) + W_{0,j}(2PC_{total\,j})^{M_j} \times (1 - PC_{total\,j}^{f_j+1} - \frac{1-PC_{total\,j}}{1-2PC_{total\,j}}) + \frac{1-PC_{total\,j}}{1-2PC_{total\,j}}}, \tag{20}$$

where M_j is the maximum number of that AC_j can double the contention-window size, $W_{0,j}$ is the minimum contention-window size of AC_j, the probability that access category j (AC_j) increase the current contention-window size is $PC_{total\,j}$, and PT_j is the probability that the back-off counter decrease by one.

4.2.3 Throughput Analysis

To derive the throughput equation for the individual access category, the probability that at least one node transmits a packet in a given back-off slot time is needed. Let PTR be the probability that at least one node transmits a packet in a certain slot time. The PTR can be expressed as

$$PTR = 1 - \prod_{j=1}^{N}(1 - \sigma_{total\,j}). \tag{21}$$

Denote P_{skj} be the probability that $k - th$ fragmented packet with access category j is successfully transmitted given the probability PTR, then, we get followings:

$$P_{skj} = \frac{N \times \sigma_{total\,j} \prod_{\beta i}(1 - \sigma_{total\,j}) \prod_{\gamma i}(1 - \sigma_{total\,j})^{\alpha_k}(1 - BER)^{kF}}{PTR}, \tag{22}$$

where N is total number of nodes, β_i is a set of contending nodes, γ_i is a set of hidden nodes, F is the size of each fragment, and α_k is the vulnerable hidden-node collision time expressed by number of back-off slots. Hence, the probability that $(k + 1) - th$ fragmented packet with access category j is unsuccessful ($P_{us(k+1)j}$) can be written as

$$P_{us(k+1)j} = (1 - \prod_{\gamma i}(1 - \sigma_{total})^{(\alpha_{k+1} - \alpha_k)}(1 - BER)^F). \tag{23}$$

By incorporating Equation 22 and Equation 23, the probability (P'_{skj}) that the $k - th$ fragmented packet is successfully transmitted and the $(k + 1) - th$ fragmented packet of access category j is failed can be represented as Equation 24.

$$P'_{skj} = P_{skj}P_{us(k+1)j}. \tag{24}$$

The P'_{S1j} means the probability of the first fragmented packet transmission with access category j is successful, and the second fragmented packet transmission is unsuccessful. And P'_{S0j} represents the probability that no packet is delivered successfully. Let T_{sj} denote be the average time that the channel is busy during successful transmission of access category j, T_{cj} as the average time that the channel is busy with unsuccessful transmission after the ACK timeout. T_{skj} is the average time that the channel is busy with successful transmission during the successful transmission of the $k-th$ fragmented packet and the failure of the $(k+1)-th$ fragmented packet of access category j. In addition, we define T_{scj} is the additional detection time when next fragmented packet is unsuccessful, and T_{ckj} is the detection time when the $k-th$ fragmented packet is unsuccessful. Then, we can express as

$$\begin{aligned}
T_{scj} &= 2(T_{PLCP} + SIFS + \sigma) + \frac{H_{mac} + F}{Data\,rate} + \frac{Ack}{Ack\,Rate} \\
T_{skj} &= 2(T_{PLCP} + \sigma) + AIFS_j + (\frac{H_{mac} + F}{Data\,rate} + \frac{Ack\,Frame}{Ack\,Rate})k + (2k-1)SIFS \\
T_{ckj} &= T_{skj} - 2\sigma, \qquad (25)
\end{aligned}$$

where T_{PLCP} is the transmission time of PLCP preambles and headers, H_{mac} is MAC header, σ is propagation time, k is the number of successful transmission packet, and $AIFS_j$ is the $AIFS$ time of access category j.

If the current fragmented packet is failed, MAC releases the channel and increases contention-window size to repeat the contending procedure. Thus, in each case, achieved throughput values are different. Let's define the throughput S_{kj}, when the $k-th$ fragmented packet is transmitted successfully, and the $(k+1)-th$ fragmented packet is failed with access category j. Using the same definition of normalized throughput, we have

$$S_{kj} = \frac{E[Payload\,Information]}{E[Length\,of\,Time]} =$$

$$\frac{PTR \times P_{skj} \times E[L]}{(1 - PTR)\sigma + PTR \times P_{skj}(T_{skj} + T_{scj}) + \sum_{i=0}^{k-1} PTR \times P'_{us\,i} T_{sc(i+1)}} . \qquad (26)$$

Therefore, the total average throughput of access category j (S_j)can be represented as

$$S_j = \sum_{i=1}^{k} \frac{P'_{S\,k\,ji}}{\sum_{j=1}^{k} P'_{S\,k\,i}} S_{k\,i} \,. \tag{27}$$

Since the throughput equation (S_j) varies upon the different number of fragments (K), and different size of fragments (F), the optimal fragmentation size (F_{OPT}) can be founded where S_j reaches the maximum value. Eventually, the maximum throughput in VANETs can be achievable based on the number of contending nodes, the number of hidden nodes, random-bit errors, and access category without protocol modifications.

4.3 System Evaluation

Network simulator 3 (NS3) is used to validate our system model. To investigate accurately the effect of access category (AC) in WAVE protocol on the fragmentation-packet size, we run two scenarios. In the first scenario, all nodes generate 1500-byte packet with the same access category (AC). Twenty nodes are distributed in the network including one hidden node, and 12 Mbps data rate is used. All nodes (including hidden node) generate either only AC3 traffic or only AC2 traffic or only AC1 traffic or only AC0 traffic with the same packet length (1500 bytes).

The average throughput using the optimal packet fragmentation is compared with the average throughput using RTS/CTS exchange under 10^{-5} BER (normal channel condition) in Figure 30. When all twenty nodes including one hidden node transmit AC0 data (general contention-window size) only, the optimal fragmentation size is 750 Byte, which means that the senders break a 1500-byte packet into two fragmented packets. Like the results in the previous chapter, because the fragmentation technique is effective for reducing the PER as well as the hidden node collision probability, the optimal fragmentation increase the network throughput by 16% compared to RTS/CTS mechanism.

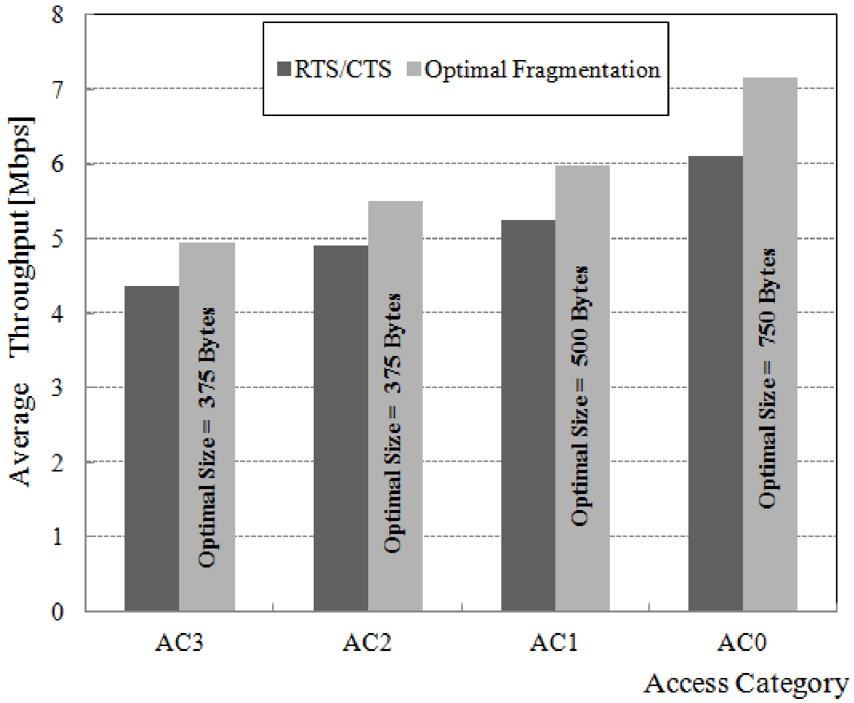


Figure 30: Throughput comparison with RTS/CTS exchange in deterministic traffic under 10^{-5} BER.

When all twenty nodes including one hidden node transmit AC3 traffic only, the optimal fragmentation size becomes 375 Byte, which means that the senders break a 1500-byte packet into four fragmented packets. Since AC3 (highest priority) has the shortest contention-window size (see Table 4) and AIFS, each node has short waiting time for the channel access and high probability that other nodes choose the same back-off slot among the contention window. Therefore, this characteristic introduces frequent collisions among the contending nodes. Moreover, the hidden node also has short contention window that induces high transmission probability. Therefore, in this environment, nodes experience severe collisions caused by both contending nodes and the hidden node. The RTS/CTS exchange can remove the hidden node collision, but it cannot remove the collision by contending nodes. Because every node exchanges the RTS and CTS signals when its back-off counter expires, if other nodes choose the same back-off slot, the RTS signal from another sender is transmitted at the same time, the RTS signal collides with another RTS signal from other sender. Therefore, RTS/CTS exchange waste bandwidth for exchanging control frames, while the transmission is still unsuccessful. Hence, the optimal fragmentation technique increases the network throughput by 14% compared to RTS/CTS by reducing the PER and hidden node collisions.

Overall, as the contention-window size becomes small, the optimal fragment size becomes short as shown in Figure 30. Generally, the optimal fragmentation performs better than the RTS/CTS exchanges. However, both RTS/CTS exchange and packet-fragmentation technique have no effect for alleviating the frequent contending node collisions resulting from the priority service with short contention-window size in VANETs.

When the channel condition becomes bad, i.e., BER is 10^{-4}, the corresponding optimal fragmentation size becomes smaller than the size under 10^{-5} BER to compensate the PER as depicted in Figure 31. The optimal fragments sizes also vary under different access category resulting from the different contention-window settings. For example, the optimal size is 500 byte for AC0 only and 256 byte for AC3 only. Since the packet-fragmentation technique is more robust to random-bit errors than RTS/CTS exchange, the improvement of the throughput is increased up to 23% than RTS/CTS in Figure 31. In this scenario, a lot of transmission failures occur because of the random-bit errors as well as severe contention between high access categories. While the RTS/CTS handshaking waste bandwidth for exchanging control signals, at the same time, they are not arrived to the receiver because of random-bit errors as well as collisions among the contending nodes, the nodes using optimal fragmentation technique experience only the collisions among contending nodes, when nodes transmit AC3 traffic only. However, these collisions are more relaxed when access category is low (AC0). Eventually, the general performance of packet fragmentation is much better than the RTS/CTS exchanges under 10^{-4} BER.

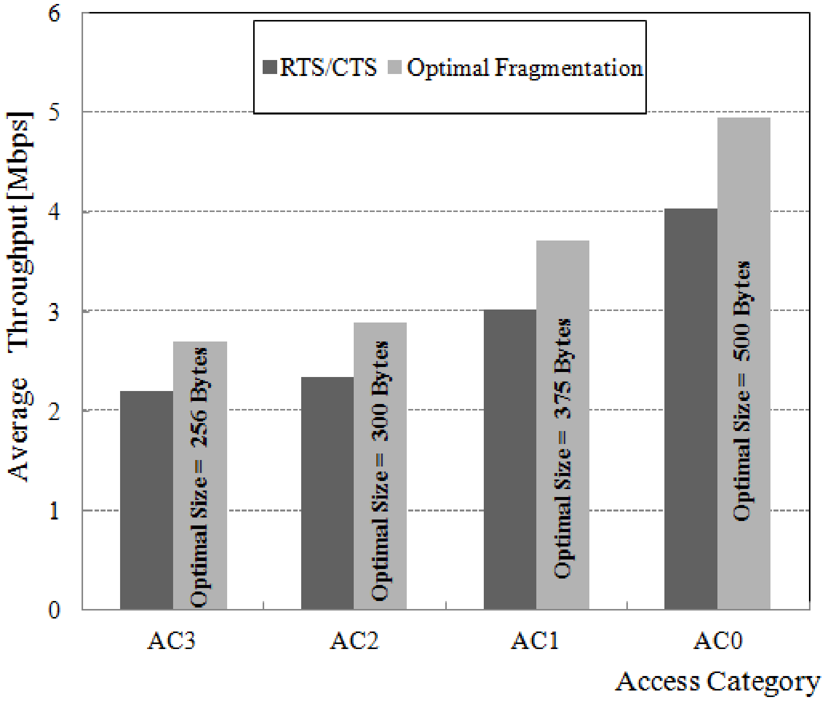


Figure 31: Throughput comparison with RTS/CTS exchange in deterministic traffic under 10^{-4} BER.

Through the above two simulation results, we showed that the optimal fragmentation technique incorporating the different contention settings for the priority service can increase the network throughput in VANETs. However, in real vehicular environments, the various applications and data types are dynamically changing, and they coexist in the network at the same time. In addition, the data patters in vehicular environment could be different from general data traffic patterns. Hence, in the second scenario, we considered more realistic traffic statistics that the size and overloads of data traffic depend on the data types such as traffic analysis statistics of CISCO company [32] in Table 5. Based on Table 5, nodes generate the corresponding access category data. One hidden node generates background data traffic in the simulation. After considering traffic statistics of CISCO company (15% video, 18% voice, 25% best effort, and 42% background), three nodes generate AC3, another three nodes transmit AC2, five nodes generate AC1, and remaining nine nodes generate AC0 traffic.

Table 5: Average data-traffic parameters form CISCO company.

Data Type	Access category	Payload size (Byte)	Packets per Second
Video	3	1400	450
Voice	2	240	33
Best Effort	1	1024	500
Back Ground	0	1500	400

Figure 32 shows the first simulation result that compares the performance between fragmentation technique and RTS/CTS exchange under 10^{-5} BER (normal channel condition). The AC1 traffic (Best Effort) takes the almost half of the bandwidth, because it generates a lot of packets per second and the total number of users is five (see Table 5).

Since the data-packet length and the number of users are different depending on the corresponding access category (AC), the optimal fragment size also varies depending on the access category. The overall throughput improvement of the fragmentation compared to RTS/CTS is roughly 20 %. In this simulation, the number of users that have short maximum contention window is 6 (AC3 and AC2), and thus, a number of contention collisions among the high access categories (AC3, AC2) is observed (but less numbers compared to two scenarios such as in Figure 30, 31). Note that the maximum contention-window size is 7 for AC3 and AC2. Since the PER is not severe under 10^{-5} BER, the fragmentation generally divides the payload into two fragmented packets. For example, the original payload sizes are 1400 byte for AC3, 1024 byte for AC1, and the optimal fragment sizes are 700 byte for AC3, 512 byte for AC1. However, the payload size for the voice traffic (AC2) is 240 byte, hence, the voice traffic does not need to be fragmented.

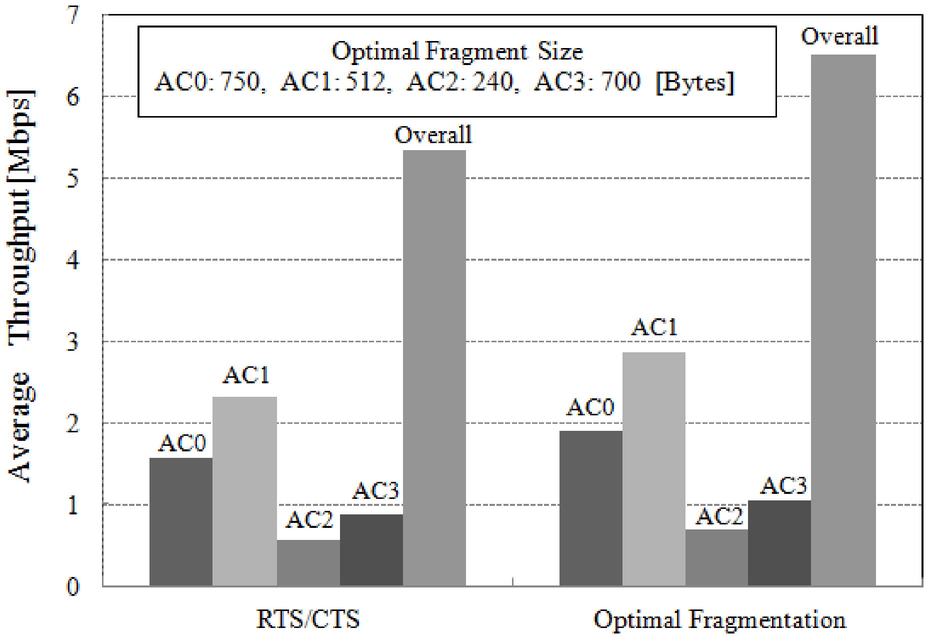


Figure 32: Throughput comparison with RTS/CTS exchange in mixed traffic under 10^{-5} BER.

Figure 33 shows the second simulation results when BER becomes 10^{-4} (bad channel condition). To alleviate the random-bit errors, the fragmentation technique chooses shorter fragment sizes compared to 10^{-5} BER channel. Rather than two fragmented packets, all access categories traffic except for the AC2 are transmitted three fragmented packets in the second scenario. For example, the optimal fragment sizes are 467 byte for AC3, 342 byte for AC1. Eventually, the overall throughput using fragmentation technique increase the network throughput by 28 % compared to the throughput using RTS/CTS exchange.

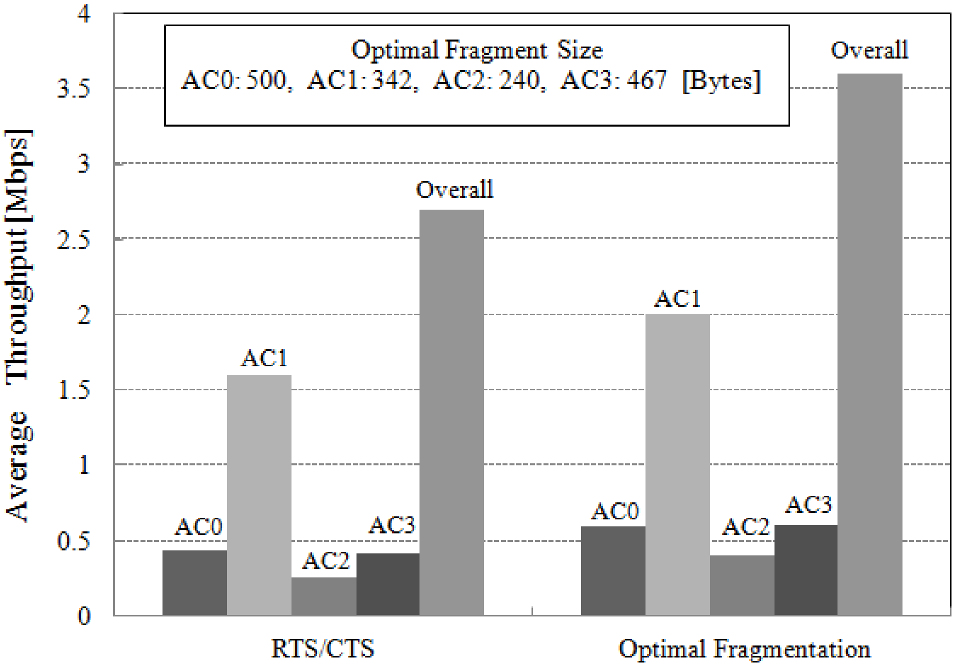


Figure 33: Throughput comparison with RTS/CTS exchange in mixed traffic under 10^{-4} BER.

4.4 Contributions and Limitations

Throughout our new Markov-chain analysis and simulations, we showed that an optimal fragmentation can also increase the network throughput under hostile channel conditions, i.e., low SNR and collisions from hidden nodes in vehicular ad-hoc networks (VANETs). The contribution of this research is to investigate the impact of the short contention-window size for the priority service with respect to the fragment lengths through theoretical analysis and simulations.

However, we found that the short contention-window setting (Table 4) for the priority service introduces severe collisions by the contending nodes. Even though only twenty nodes are distributed in our simulations, as depicted in Figure 30 and 31, twenty nodes that have AC3 traffics degrade the performance. Unfortunately, the optimal fragmentation and

RTS/CTS have no effect to avoid this collision, which is a fundamental nature of WAVE protocol. Since the WAVE protocol is designed for the priority service, the solution for this problem should not degrade the priority performance of WAVE protocol. Therefore, we will focus on this severe contention problem in the next chapter.

CHAPTER 5

DYNAMIC SERVICE-CHANNEL ALLOCATION (DSCA)

Providing tools to achieve a high level of safety transportation is the important objective in Vehicular Ad-hoc Networks (VANETs) research. Hence, most of the works are devoted to developing safety-message dissemination algorithms. However, non-safety applications can also contribute to the network efficiency by exchanging traffic information. To support these applications, VANETs adopt the wireless access in the vehicular environment (WAVE) to guarantee the quality of service (QoS) using four different access categories. However, the WAVE could not provide the QoS to the users due to the collisions caused by the small contention-window size for the top priority traffic, when top-priority traffic is dominant. Therefore, this small contention-window size setting for the prioritization induces severe performance degradation. In this chapter, the Dynamic Service-Channels Allocation (DSCA) method is proposed to maximize throughput by dynamically assigning different service channels to the users.

The remainder of this chapter is organized as follows. A motivation, problem description, and related works for the chapter are given in Section 5.1. Section 5.2 explains Dynamic Service-Channels Allocation (DSCA) algorithm with analysis. Extensive simulation results are presented in Section 5.3. In the last section, we also discuss about the implementation issues of DSCA and conclude the chapter by discussing.

5.1 Motivation and Related works

5.1.1 Channel-allocation Problem

The IEEE 802.11 standard defines multiple channels to increase network throughput. The conventional multi-channel allocation usually focused on minimizing adjacent channel interferences and maximizing spatial reuses based on geographical location in cellular networks as well as in the IEEE 802.11 networks. However, in VANETs, high mobile stations (vehicles) keep changing the network topology frequently. Hence, the precise geographical location information should be updated periodically. Note that exchanging all location information requires channel resources, and that frequent changing current channel to different channel requires switching costs such as synchronization overheads [**?**]. Therefore, channel allocation scheme in VANETs must be treated in a different way.

In vehicular ad-hoc networks (VANETs), the control-channel access and its short duty cycles with service-channel access lead many researchers to focus on the safety message exchange schemes for the vehicle accident, which is a fundamental nature of VANETs. Because the safety message should be delivered to all sender's neighbors and to the following vehicles with minimum delays [33], several studies investigated the broadcasting schemes in [34], [35], [36] and [37] etc. Theses researches not only focus on the analysis of current broadcasting structures [35], but also suggest that how to organize the multi-hop broadcasting procedures efficiently with minimum delays, and without collisions and broadcasting storms [36] in a common control channel (CCH).

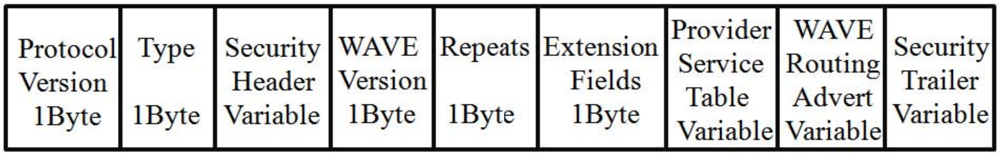
On the other hand, utilizing the service channels (SCHs) has not much been investigated compared to the control-channel utilization, although service channel could contribute entire network efficiency in VANETs. The enhanced distribution channel access (EDCA) used in the SCHs (Service Channels) is designed for time-critical messages such as real-time video data. The four different access categories with different contention-window sizes provide the priority service as described in the previous chapter. However, this prioritization scheme does not guarantee QoS of non-safety messages in dense traffic conditions [38], because the limited contention-window sizes for the prioritization in high access categories increase collision probability significantly. In such a dense traffic situation, the vehicles should be well-distributed over the four available service channels so that each channel does not waste of its bandwidth from the collisions. However, there is little attention for channel-distribution technique to maximize the service-channel resources.

5.1.2 Current Multi-channel Operation in Service Channels

In vehicular ad-hoc networks (VANETs), any node or RSU (Road Side Unit) that wants to provide services on service channels in next SCH intervals, should announce the availability using WAVE service advertisements (WSA) during the preceding CCH interval [39]. If other nodes receive interesting advertised services, they would switch to relevant service channels (SCHs) after CCH interval. Otherwise, they remain in the current control channel. This advertising service may take one service interval or more than one service interval.

In the WSAs format (Figure 34), it has mandatory 1-byte repeats field, which indicates how many times this WSA is advertised in each 100 ms sync period. This WSA, which includes both service information and the advertising-channel information, is repeatedly sent to neighbor nodes several times. Hence, not only it increases the successful advertisement probability, but also it can be used as one of the measurement of link quality, even though it might not good indicator of link quality in service channels [39]. In WSAs header extension field, it includes transmitted powers, 2D or 3D locations. The other service provider table field indicates 1-byte service priority from AC0 to AC3, 1-byte service channel number, 1-byte data rate, provider service context and so on as shown in Figure 34.

However, current protocol does not specify that how to assign their service channels. Every service channel could have different interferences, path loss, and data service traffics. Besides, these parameters keep changing because of the dynamic channel environments in VANETs. Moreover, each node might have different kinds of services in dense traffic environments. This means that each service uses different access categories, which are designed for priority services. However, high access categories such as AC3 and AC2 have short window size (Table 4), which cause severe collisions among them, and thus, leads significant performance degradations.



Protocol Version	Type	Security Header	WAVE Version	Repeats	Extension Fields	Provider Service Table	WAVE Routing Advert	Security Trailer
1Byte	1Byte	Variable	1Byte	1Byte	1Byte	Variable	Variable	Variable

Figure 34: WAVE service advertisement (WSA) format.

5.1.3 Related works

A channel-utilization problem in VANETs is critical, since safety-message broadcasting in CCH and real-time data packets in SCHs require minimum delays and QoS (Quality Of Services), simultaneously. This channel-utilization topic can be categorized into two different areas: One is multiple channel-access problem of single channel, and the other is channel-allocation problem of four SCHs.

The multiple access and channel coordination based on the cognitive MAC protocol for VANETs (CMV) is proposed using both short-term spectrum sensing and long-term spectrum sensing in [40]. In [40], devices classify the service-channel status based on the received signal strength (RSS) values from spectrum sensing every 1 ms. Moreover, it also uses wide band spectrum-pooling technique for channel access based on the short-term spectrum access. However, CMV requires protocol modification of MAC layer in VANETs. It also underestimates the effect of multiple transceiver co-interferences. Furthermore, installing multiple radios in vehicles costs additional expenses, because hardware constraints of cognitive radio and cross-channel interferences between radios make it hard to deploy in real devices. Hence, the impact of sensing overhead for multi-channel allocation should be considered [41], a hardware-constrained cognitive MAC is proposed for the efficiency of spectrum sensing and spectrum-access decision in [41].

On the other hand, current multi-channel coordination works in VANETs can be accomplished by either distributed or centralized ways, with or without road side units, using single or multiple transceiver, and through control channel or not. In [42], the authors proposed channel allocation schemes for routing to reduce interference between nodes. Every node stores the received signal strength from its neighbor nodes and evaluated SIR (Signal to Interference Ratio), if a channel is available. If the channel satisfies target SIR value, then the sender switches to the channel. However, as a result of the characteristic of VANETs (the simulation results are highly dependent on the simulation topology), more simulations under dynamic channel environments and theoretical analysis are required in [42]. Moreover, how to manage the target SIR value in real-time remains as a future work. A vehicular mesh network (VMESH) is proposed in [43] by incorporating the effects of alternate access between CCH and SCHs in WAVE system. Using several beacon slots for a synchronized distributed beaconing protocol, mobile nodes can reserve the channel based on the time division multiple access (TDMA). This VMESH divides the CCH interval into two periods, which are beacon period and safety periods. During this beacon periods, nodes negotiate the channel resource reservation. The limitation of this paper lies on the assumption that this reservation process must be completed with no transmission failures. Similar idea of splitting CCH intervals for multiple access and channel coordination can be found in [44]. In [44], the authors also divide the CCH interval into adaptive broadcasting periods and contention based reservation periods for channel access. However, these algorithms, sharing CCH intervals with channel coordination may reduce the successful probability of safety message exchanges, and thus, it does not guarantee passengers safety, which is the critical objective of VANETs. All above proposed protocols used decentralized channel access and allocation schemes.

In other respects, VANETs also have a road side unit (RSU) to support network-access point as an infrastructure. A RSU centric channel-coordination protocol is proposed in [45]. A vehicle sends channel-request packets to a RSU, which contain transmission information in the vehicle through the control channel. The RSU keeps tables, which contain the channel information that assigned to particular vehicle for channel access. However, this work has limitation of using control channel for channel request packets, and it also need the RSU to operate this protocol. The authors also simulated under sparse traffic as only 20 vehicles. However, in the congested highways, there could be more than 40 vehicles within 250 meters of transmission range. Similarly, a RSU assisted multi-channel coordination MAC (RAMC) protocol is suggested in [46]. The authors incorporated realistic channel model which is Nakagami model with m=3, and RAMC also sends single safety message via control channel with various traffic densities. By sacrificing that a road side unit (RSU) monitors all the safety messages, a vehicle can achieve high throughputs for non-safety messages. Nevertheless, RSU's aid is also necessary in this research.

5.2 Dynamic Service-Channel allocation (DSCA) in VANETs

5.2.1 Algorithm Description

The dynamic service-channel allocation (DSCA) is targeting realistic VANETs environments as follows:

- The vehicle density could be high enough to induce frequent collisions in both a control channel and service channels.
- Every vehicle has different access categories (AC) to provide services in service channels.
- Control channel is used severely for the safety-message broadcasting and other control messages.
- Random-bit errors (BER) and hidden-node collisions occur during the transmission.

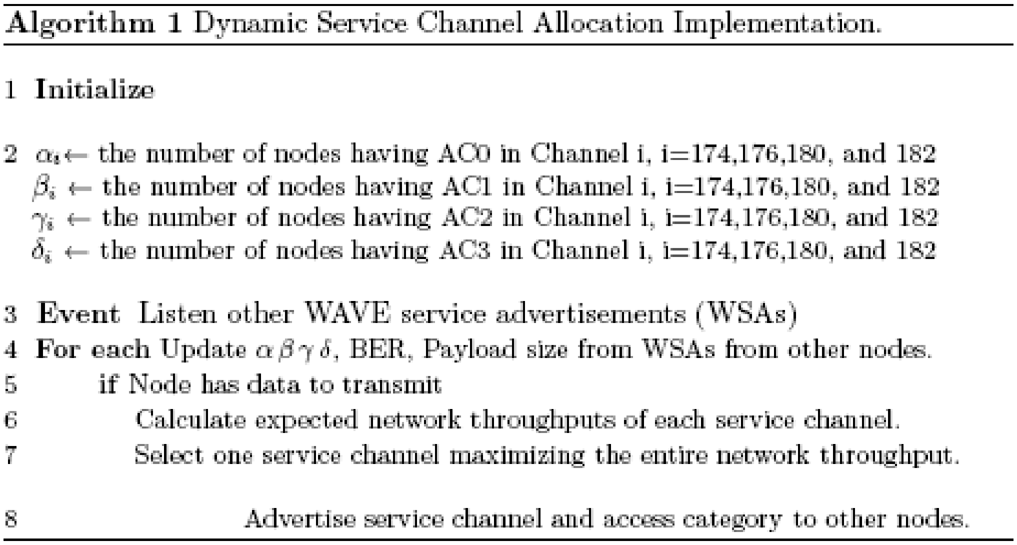
In these environments, exchanging additional channel information for the multi-channel allocation through control channel makes the channel conditions worse, because it uses limited-channel resources. As a result of frequent transmission failure by the collision and interference, these channel-information exchanges may not succeed during the control-sync interval. Unlike most of existing channel-allocation strategies, the DSCA does not require the additional exchanging information. The DSCA uses the existing channel information and service information through WSAs.

The key idea of DSCA is to achieve maximum network throughput in four service channels by assigning different nodes for the available service channels based on the current access categories from AC0 to AC3 (see Table 6). More specifically, before each vehicle (that wants to provide services during next service-channel interval) announces its service-channel number during the preceding control-channel interval, it calculates the expected throughput in the specific service channel (i.e., SCH 174 or 176 or 180 or 182) to maximize the entire network throughputs based on current information that is received through the past WSAs advertisements. For example, if a vehicle has a access category X (ACX) packet to send, it calculates the expected throughput when it joins the specific service channel based on the current number of users in each channel. Let the number of users with AC0 in SCH 174 be α_{174}, the number of users with AC1 be β_{174} , the number of users with AC2 be γ_{174}, and the number of users with AC3 be δ_{174} as summarized in Table 6.

Table 6: Number of vehicles based on the access category in each service channel.

	AC0	AC1	AC2	AC3
SCH 174	α_{174}	β_{174}	γ_{174}	δ_{174}
SCH 176	α_{176}	β_{176}	γ_{176}	δ_{176}
SCH 180	α_{180}	β_{180}	γ_{180}	δ_{180}
SCH 182	α_{182}	β_{182}	γ_{182}	δ_{182}

After this vehicle selects one of the available service channels based on these parameters, it advertises the specific service-channel number and current access-category number by the standard. The next vehicle that will provide services updates the current channel information based the WSAs from the previous node and updates the corresponding parameters (α, β, γ, $and\, \delta$) as depicted in Figure 35. Because each vehicle selects the best channel in a distributed manner, DSCA does not require any central coordinators. Even if one vehicle does not get the correct channel information due to the noisy environments, it may update the parameters (α, β, γ, *and* δ) based on the wrong channel information. Therefore, the vehicle selects and advertises the incorrect channel number through WSAs. However, the following vehicle could find the best channel based on the accumulated channel information from the WSAs sent by all other nodes. As a result, a misjudgment of single vehicle does not induce the entire performance degradation. To summarize, our key idea lies on that the proper relative percentage of four different access categories increase the entire network throughput by avoiding severe contentions of different access categories.



Algorithm 1 Dynamic Service Channel Allocation Implementation.

```
Initialize

$\alpha_i \leftarrow$ the number of nodes having AC0 in Channel i, i=174,176,180, and 182
$\beta_i \leftarrow$ the number of nodes having AC1 in Channel i, i=174,176,180, and 182
$\gamma_i \leftarrow$ the number of nodes having AC2 in Channel i, i=174,176,180, and 182
$\delta_i \leftarrow$ the number of nodes having AC3 in Channel i, i=174,176,180, and 182

Event  Listen other WAVE service advertisements (WSAs)
For each Update $\alpha \beta \gamma \delta$, BER, Payload size from WSAs from other nodes.
    if Node has data to transmit
        Calculate expected network throughputs of each service channel.
        Select one service channel maximizing the entire network throughput.

                Advertise service channel and access category to other nodes.
```

Figure 35: DSCA algorithm.

5.2.2 System Analysis

Our throughput analysis is based on the analysis in Chapter 4 using Markov-chain model [31] to incorporate the WAVE characteristics in VANETs. However, the authors in [31] assume that every node transmits different access categories randomly, because their work is based on the IEEE 802.11e EDCA. However, in VANETs, nodes can exchange their services and corresponding access categories through WSAs in every sync interval, hence, other nodes can get the access-category information. Therefore, our analysis also considers that each node could have one deterministic access category as well as random access categories with different packet lengths.

We assume that there are N_{total} vehicles that want to provide services in the networks, and N_{ACi} is the number of vehicles that currently have packets of $i-th$ access category to send in a current slot time after the internal contention (either random traffic or deterministic traffic). Therefore, the total number of vehicles N_{total} can be expressed as

$$N_{total} = \sum\nolimits_{i=0}^{3} N_{ACi}. \tag{28}$$

The number of vehicles in the specific channel (SCH 174, SCH 176, SCH 180 and SCH 182) based on the Table 6 can be expressed as

$$\begin{aligned} N_{174} &= \alpha_{174} + \beta_{174} + \gamma_{174} + \delta_{174} \\ N_{176} &= \alpha_{176} + \beta_{176} + \gamma_{176} + \delta_{176} \\ N_{180} &= \alpha_{180} + \beta_{180} + \gamma_{180} + \delta_{180} \\ N_{182} &= \alpha_{182} + \beta_{182} + \gamma_{182} + \delta_{182}. \end{aligned} \tag{29}$$

where $N_{CH\#}$ is the total numbers of vehicles in each service channel, and N_{ACi} can be represented as

$$\begin{aligned} N_{AC0} &= \sum\nolimits_{all\,channels} \alpha_i \\ N_{AC1} &= \sum\nolimits_{all\,channels} \beta_i \\ N_{AC2} &= \sum\nolimits_{all\,channels} \gamma_i \\ N_{AC3} &= \sum\nolimits_{all\,channels} \delta_i. \end{aligned} \tag{30}$$

Note that the authors in [31] assumed that all nodes have four different access-categories data, and each access-category data competes for the internal contention. Our analysis also considered that each vehicle has one deterministic access-category data. Moreover, the highest priority is AC0 in [31], but in this analysis, AC3 is highest priority-access category as same as the WAVE priority in VANETs. Therefore, the internal collision probability (PI_i) of the random traffic should be

$$\begin{aligned}
&PI_0 = 1-(1-\tau_3)(1-\tau_2)(1-\tau_1)\\
&PI_1 = 1-(1-\tau_3)(1-\tau_2)\\
&PI_2 = \tau_2\\
&PI_3 = 0\\
&\delta_0 = \tau_0(1-\tau_3)(1-\tau_2)(1-\tau_1)\\
&\delta_1 = \tau_1(1-\tau_3)(1-\tau_2)\\
&\delta_2 = \tau_2(1-\tau_3)\\
&\delta_3 = \tau_3 \qquad\qquad ,
\end{aligned} \tag{31}$$

where $\sigma_{total} = \sum_{i=0}^{3}\sigma_i$. The transmission probability of access category AC_i for the single station is denoted as σ_i, and τ_i is transmission probability of AC_i in the internal contention in [31]. If each node has a deterministic access category, then, all the internal collision probability become zero, which means $PI_0 = PI_1 = PI_2 = PI_3 = 0$ and $\delta_i = \tau_i \, for\, every\, i.$ We also consider that each service channel could have different average random-bit error rate (BER), so we denote average BER of each service channel as BER_{CH174}, BER_{CH176}, BER_{CH180} and BER_{CH182}. The external collision probability (PO) by incorporating BER effects can be written as

$$PO = 1 - \prod_{N_{SCH}} (1-\delta_{total\, node\, i})(1-BER)^{Payload size\, of\, AC}, \tag{32}$$

where N_{SCH} is the number of nodes in a current service channel, which can be N_{CH174}, N_{CH176}, N_{CH180} or N_{CH182} . PT_i denotes the probability that the back-off counter of AC_ican be successfully decreased by one slot time. Based on the Equation 31, 32, and 20, we can get both τ_i and δ_i using numerical analysis.

To get the saturation throughput, we need the probability that at least one node transmits a packet in a given slot time (PTR). By incorporating both random traffic case and deterministic case, our new PTR is

$$PTR = 1 - \prod_{all\,nodes} (1 - \delta_{total\,node\,i}). \tag{33}$$

After considering the channel BER effect, the probability of success transmission of access category (AC_i) can be expressed as

$$PS_i = \frac{N_{SCH}\delta_i(1 - BER_{CH})^{E[L_i]} \prod_{except\,i}^{all}(1 - \sigma_{total\,node})}{PTR}, \tag{34}$$

where $E[L_i]$ is average packet length of access category i .

Finally, the saturation throughput of access category i (AC_i) can be expressed as

$$S_i = \frac{PS_i\,PTR\,E[L_i]}{(1 - PTR) + PTR\sum_{j=0}^{3} PS_i\,t_{s_j} + PTR\,PFC\,t_c}, \tag{35}$$

where the unsuccessful transmission probability (PFC) due to the collisions and BER, and $PFC = 1 - PS_i$, $E[L_i]$ is average packet length of access category i , t_c is collision detection time, and $t_{s_j}$is the successful transmission time of access category j. By summation the saturation throughput over the four access categories, We can get the current channel throughput $S_{CH\#}$, which is

$$S_{CH\#} = \sum\nolimits_{i=0}^{3} S_{CH\#\_ACi}. \tag{36}$$

And the aggregated network throughput over the four service channels should be

$$S_{total} = \sum\nolimits_{all\,channels} S_{CH\#}. \tag{37}$$

Among the throughput under different α, β, $\gamma\, and\, \delta$, we can adjust the number of access categories (α, β, $\gamma\, and\, \delta$) so that the entire network throughput reaches the maximum.

5.3 System validation

5.3.1 Simulation Setup

NS3 simulator is used to validate our system model, TraNS (Traffic and Network Simulation Environment) is used for the traffic mobility. To incorporate realistic simulation parameters, we used general traffic data statistics based on the traffic analysis (Table 5) from CISCO Inc. Because of the short window size and arbitration inter-frame space number (AIFSN) for high priority-access category, AC3 traffic will take almost the entire bandwidth, while low access-category traffic can access the channels with minor probability. Therefore, we generate the each traffic randomly so that total generation time is 60 seconds during 180 seconds simulation time. Moreover, considering the vehicle-traffic density within a transmission range, we changed the number of vehicles from 100 to 500. In Table 7, we summarized simulation parameters. Because our model considers the random traffic load as well as the deterministic traffic load, we run two scenarios in our simulations.

Table 7: Simulation parameters.

Data frame retry count limit	5
Control frame retry count limit	7
Total Number of Vehicles	100, 200, 300, 400 and 500
BER	10^{-6} to 10^{-4}
Data Rate	12 Mbps
Slot Time	13 µs
Propagation Delay	1 µs
$CWIN_{min}$& $CWIN_{max}$	31 & 1023
Simulation Time	180 seconds
Transmission Range	300 m
Propagation Model	Nakagami
SCH Interval & CCH Interval	50 msec (each)
Vehicle Velocity	40 to 60 miles / hour (Avr. 50)

5.3.2 First Scenario (Deterministic Traffic Loads)

In the first scenario, we used the deterministic traffic loads (15% video, 18% voice, 25% best effort, and 42% background) based on Table 5. For example, if the total number of vehicles is 100, then 15 vehicles provide video-traffic services, and 18 vehicles provide voice over ip traffic, and so on. We keep changing the average BER from 10^{-6} to 10^{-4}, which generally represent good channel conditions and bad channel conditions, respectively.

Figure 36 shows the overall simulation results of Scenario one. Even-though video traffic takes only 15% of the entire traffics, due to the short contention-window size and short AIFSN, it takes most of the bandwidth during the entire simulation time. The average throughputs with DSCA per a service channel are compared with the uniform channel allocation in the Figure 36. Overall, the DSCA performs better than uniform channel allocation over different vehicle densities and BERs.

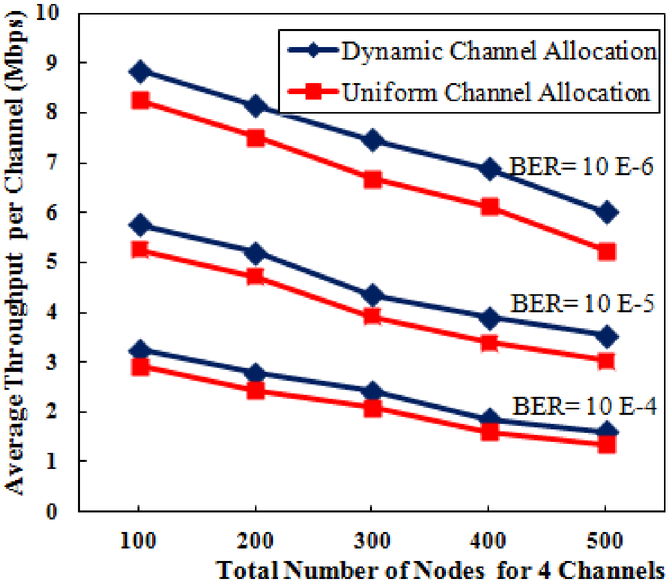


Figure 36: Overall average throughput comparison in the first scenario.

We observed that the throughput improvement percentage using DSCA keeps increasing rather than the uniform channel allocation, when the number of nodes is increasing (Figure 37). When total number of nodes is 100, the actual number of video traffic nodes is just 15 over the 4 service channels. Therefore, the DSCA improves the average throughput per channel from only 7% to 11% over various BERs in Figure 37. However, as the number of vehicles increases up to 500 vehicles in 4 service channels, the enhanced percentage keep increasing, and thus, we can achieve 19 % improvement of the average throughput than the uniform allocation. Moreover, when the channel condition becomes worse (i.e, BER increases), the improvement percentage slightly increases. Because the video traffic usually has longer payloads (1400 byte) than other packets, the transmission by the video traffic (AC3) nodes could not succeed well due to the high PER. To make matters worse, those nodes have short contention-window size (note that maximum contention window size for AC3 is 7). Hence, they waste most of the transmission time not only for the contentions among them, but also for the errors by PER.

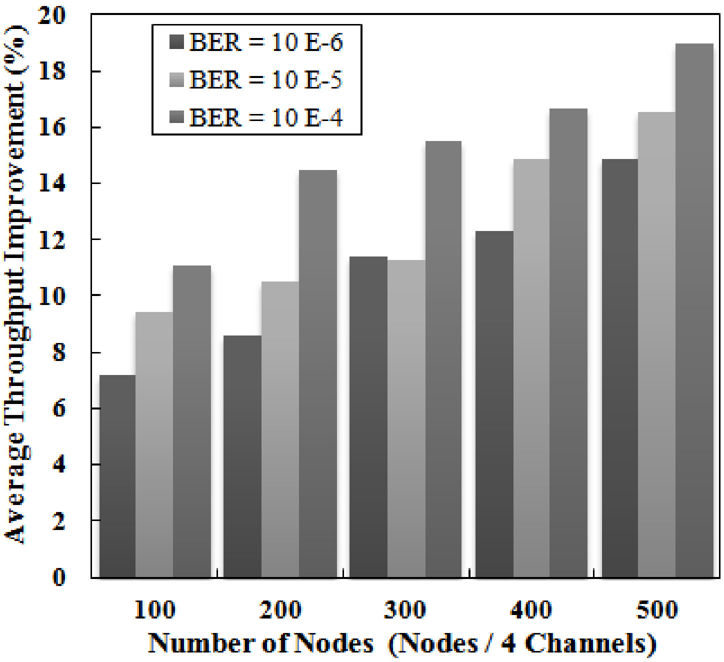


Figure 37: Throughput improvement percentage in the first scenario.

Figure 38 shows the comparison of each access-category throughput between uniform channel allocation and DSCA, when channel condition is good, e.g., BER is 10^{-6}. In uniform allocation, nodes that have low priority (AC1 and AC0) have little chances for the channel access. The nodes that have higher priority always use the channel, while low priority nodes also contend with the other nodes that have same low priority. Hence, the throughput of AC0 stays almost zero in the uniform allocation. However, in the DSCA, even the AC0 node has some chances to access the channel with small portions. For example, while uniform allocation assigns four AC3, four AC2, six AC1 and ten AC0 traffics in SCH 176 (Note that N_{AC3} is 15, N_{AC2} is 18, N_{AC1} is 25, and N_{AC0} is 42 when total number of vehicle is 100) our dynamic scheme allocates two AC3, two AC2, seven AC1, and twelve AC0 traffics. Hence, AC0 traffic in DSCA could access the channel due to less competition with AC3.

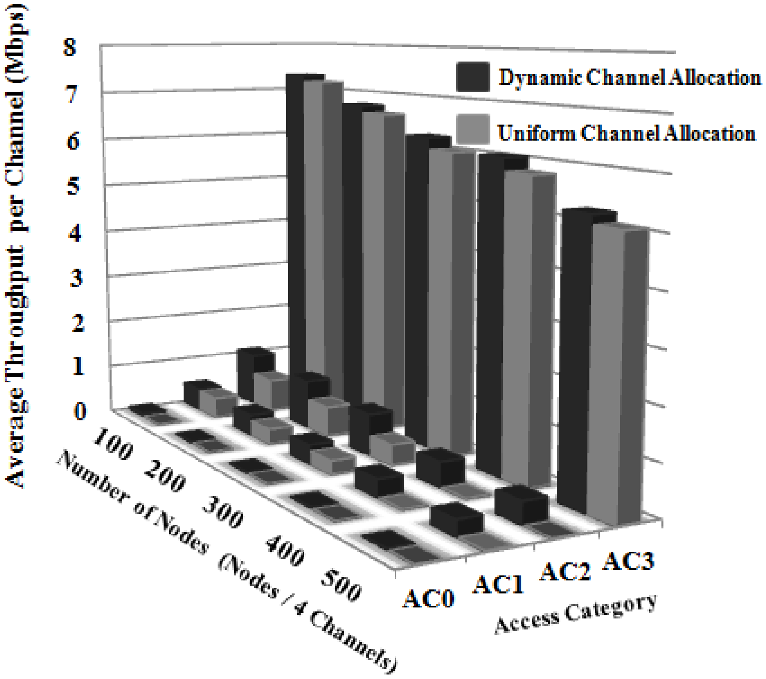


Figure 38: Relative AC ratio (BER = 10^{-6}) in the first scenario.

As the channel condition deteriorates (BER of 10^{-5}or 10^{-4} as shown in Figure 39 or 40), the AC2 that has the shortest payload length (250 Byte) could have better success transmission probability due to the low PER. Therefore, the percentage of AC2 traffic contributing the throughput is increased. However, note that the DSCA still yields more throughputs in both AC2 and AC3 than the uniform allocation approach, and only the ratio of AC2 to the total throughput has been increased.

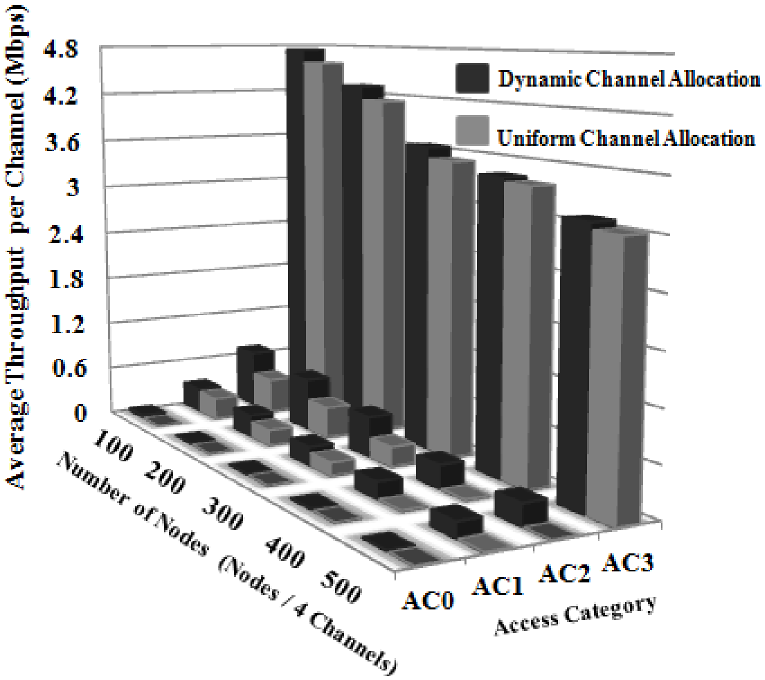


Figure 39: Relative AC ratio (BER = 10^{-5}) in the first scenario.

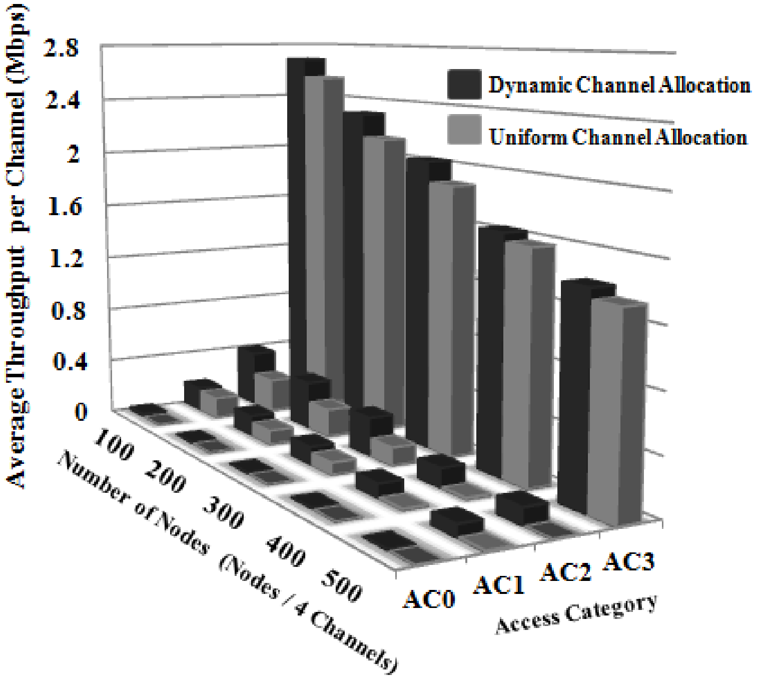


Figure 40: Relative AC ratio (BER = 10^{-4}) in the first scenario.

5.3.3 Second Scenario (Random Traffic Loads)

If every vehicle generates four different types of access category traffics based on the Table 5, due to the internal contention, AC3 and AC2 always win the internal contention inside the node. Therefore, almost all nodes have either AC3 or AC2 traffics in this environment. To avoid channel access by only AC3 and AC2, all nodes generate four different types of traffic with equal probabilities in random order. Even though they choose one access-category traffic and put it in the queue, because different access categories use different queues, they still experience the internal contentions. Figure 41 shows the overall result in the second scenario.

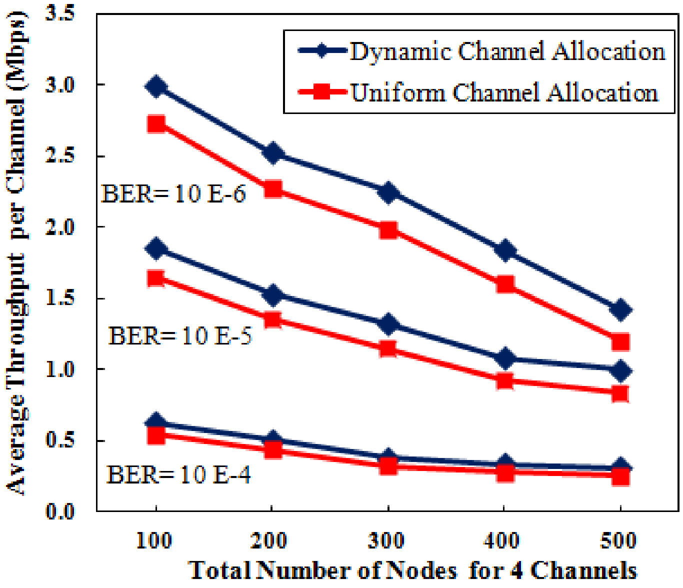


Figure 41: Average throughput comparison in the second scenario.

Because of the internal-contention procedure, the average contention-window size in the second scenario is more inflated than the first scenario. If the high priority data and low priority data collide internally, the high priority data wins. Hence, high priority node prepares the general CSMA/CA procedure, while low access category node increases the contention-window sizes. Therefore, the total number of AC3 and AC2 is greater than the first scenario, and the total number of AC1 and AC0 is decreased. Due to the increased number of AC3 and AC2 traffic and their short contention-window sizes, the collision probability becomes bigger than Scenario one. Hence, numerous retransmission procedures of AC3 accounted for the most of the transmission time. Consequently, the average throughput in second scenario is much less than the average throughput in first scenario as depicted in Figure 41.

The average throughput of DSCA compared to the uniform channel allocation is also increased from 9% up to 22%, when BER becomes worse (see Figure 42).

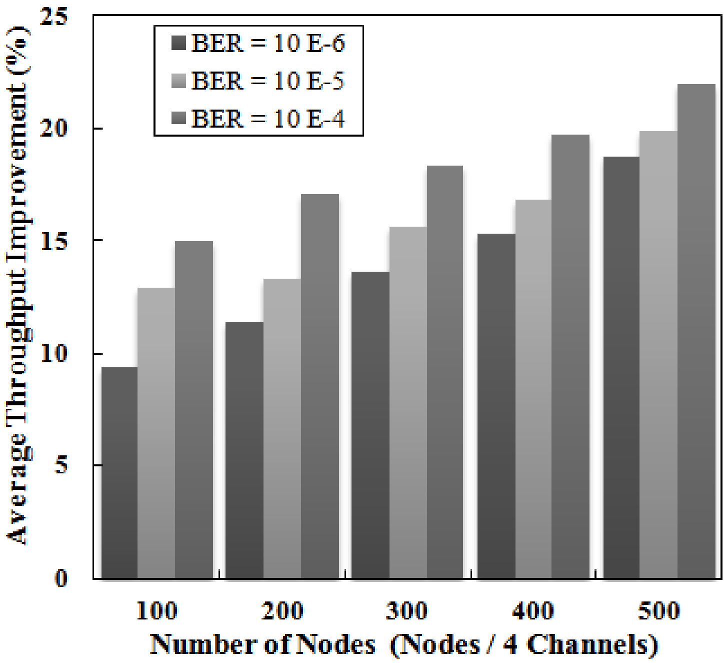


Figure 42: Throughput improvement percentage in the second scenario.

Furthermore, our DSCA allows more throughput of AC2, AC1, and AC0 traffics than the uniform channel allocation. When the channel condition becomes worse (i.e. BER = 10^{-4}), AC2 that has lowest PER by short payload (see Table 5) has better successful transmission probability than others. Hence, the relative throughput ratio of AC2 is bigger than the good channel condition (i.e. BER = 10^{-6}) as shown in Figure 43, 44, and 45.

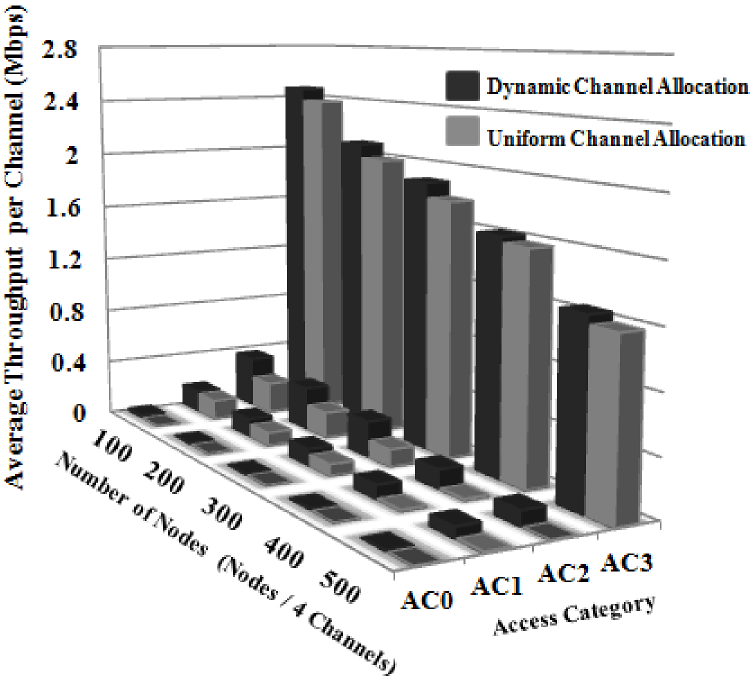


Figure 43: Relative AC ratio (BER = 10^{-6}) in the second scenario.

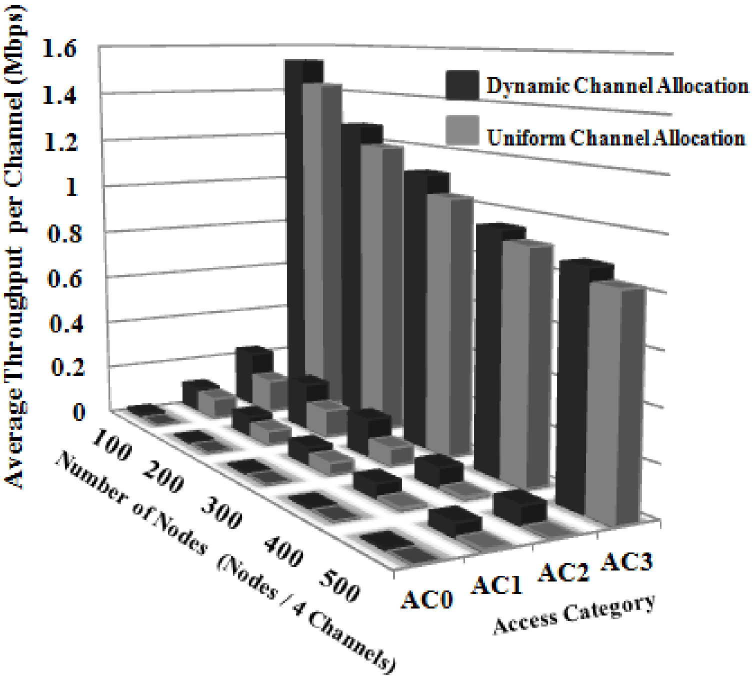


Figure 44: Relative AC ratio (BER = 10^{-5}) in the second scenario.

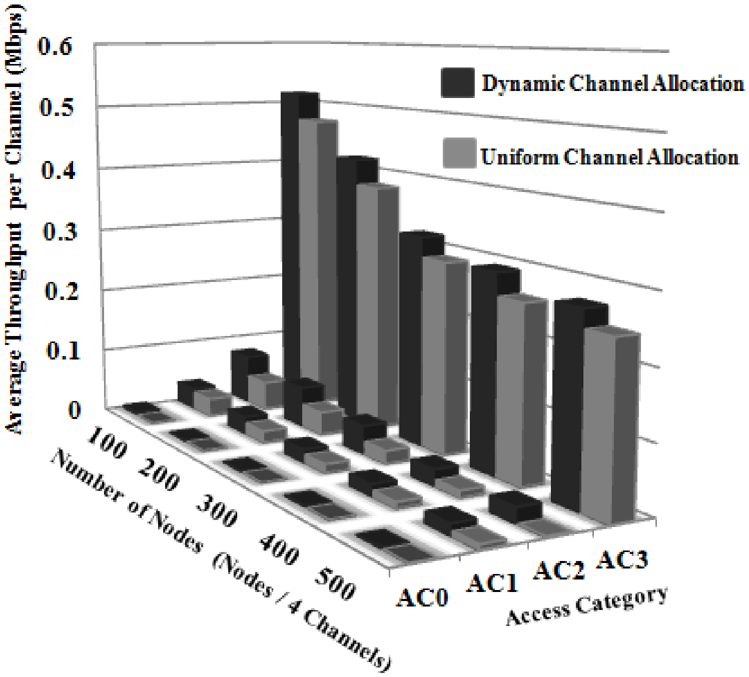


Figure 45: Relative AC ratio (BER = 10^{-4}) in the second scenario.

To summarize based on the two scenarios, our dynamic channel allocation (DSCA) not only increases the entire network throughput, but also allows nodes that have low access-category traffic to access the channel. Furthermore, our scheme also increases the throughput of highest access category under various channel conditions.

5.4 Contribution of DSCA and Conclusions

5.4.1 Benefits of DSCA

In this sub-chapter, we listed the advantages of our DSCA algorithm.

- No impact on the performance of safety applications: The safety message dissemination to neighbor nodes in VANETs requires minimum delays and efficient multi-hop broadcasting to the nodes, which are out of transmission ranges. However, excessive collisions of broadcasting messages as a result of dense vehicle traffics, severe bit-error rate by high mobility, interference and obstacles [47] deteriorate the safety broadcasting performances seriously. Moreover, as a result of alternating short CCH interval (50 m sec) with SCH interval and basic safety message from each vehicle per 100 m sec sync period by standard, the control channel could be extremely busy. In such environment, exchanging additional information for multi-channel coordination during CCH interval might not only waste the bandwidth, and thus, induces the performance degradation of safety message dissemination, but also the information could not be delivered to the destinations. Since no additional message exchanges are required in our scheme, it does not affect the performance of the non-safety applications.

- No protocol modifications and no multiple antennas: Our scheme is based on the general WAVE service advertisements (WSAs), and thus, does not require any protocol modifications. To the best of our knowledge, any modified protocol could bring undesirable problems. In addition, even though the standard allows to use multiple transceivers (not mandatory) [28], the current protocols do not provide a way for one device to determine how many antennas neighbor nodes have [39]. Considering the complexity for implementation of multiple transceivers as well as co channel interference because of asynchronous transmission [48], our scheme based on the assumption that each device has one transceiver would be more desirable in real VANETs environments. Moreover, most of VANETs device manufacturers who finished their prototype of 802.11p wireless module such as [49], does not consider multiple transceiver because of the additional cost and complexity. They also have a global positioning system (GPS) that requires extra costs. On the other hand, directional antennas can be used for solving multi-channel problems [50], however, the deafness problem [51] using directional antennas might be fatal to the safety applications.

- No central coordination: Our dynamic multi-channel scheme does not require central coordinator for assigning appropriate service channel numbers to the nodes. Generally, the central coordinator is often difficult to respond appropriately to dynamic vehicular environment. Moreover, it needs entire channel information from every node in the network, and it might fail to get correct channel information in a short time when channel is crowded with many vehicles. Even if the central coordinator could receive all the information in proper time, how to choose efficiently the coordinator must be investigated in high mobile environments. Therefore, optimal channel allocation might not be achievable in real vehicular environments, and thus induce performance degradations. On the contrary, our scheme calculates and selects the best channel number based on the updated WSA from other nodes. Hence, even though one node selects a wrong channel because of the excessive collisions of WSA or other reasons, the following node could select the best channel again to maximize the entire network throughput based on this WSA from the previous node. Therefore, misbehavior of one node does not affect on the entire network performance.

5.4.2 Conclusion

In this chapter, the dynamic service-channels allocation (DSCA) method is proposed to maximize throughput by dynamically assigning different service channels to the users. The solution for assigning multiple service-channels is based on the realistic assumptions in vehicular environments that include BERs, different access categories, and dense traffic conditions using single transceiver. DSCA is thoroughly analyzed based on Markov-chain model under the saturation conditions. To show the feasibility of DSCA, realistic parameters are used from the CISCO traffic statistics in NS-3 simulation. The average throughput is evaluated extensively under various channel conditions and vehicle densities. Moreover, both randomly generated and deterministically chosen traffic are studied. As a result, the proposed DSCA enhances the average network throughput by 19% in deterministic access category scenario and by 22% in random access category scenario. DSCA also reduces the collision probability of high priority-access category packets, such as video and voice data, and thus, improves QoS of real-time traffic. The major contribution of this work is that DSCA can enhance throughput without the need for protocol modifications, multiple antennas, and the central coordination. DSCA does not sacrifice the performance of safety applications to solve multi-channel allocation problem in realistic VANETs environments. Moreover, inaccurate channel allocations will not degrade the performance due to the dynamic nature of selecting new optimal values in the DSCA algorithm.

By the the IEEE 802.11p standard, every node should transmit periodic broadcasting messages (beacon messages) including location, node id, velocity, direction and so on. Hence, they can announce their presence in the network, at least every one seconds (1Hz). However, how frequently these beacon messages should advertise does not specified in the protocol. Usually, researchers expect the frequency range form 1 Hz to 10 Hz. Since each vehicle can exchange service information including packet size and corresponding access categories (AC) through WSAs in every sync interval, neighbor nodes can update the current channel information. Therefore, DSCA algorithm can be easily implemented in VANETs.

CHAPTER 6

CONCLUSIONS AND FUTURE WORK

In this dissertation, we have created a framework for improving the performance of mobile ad-hoc networks (MANETs) as well as vehicular ad-hoc networks (VANETs). Overall, the contributions of this thesis are illustrated in Figure 46. Specifically, we propose two techniques that do not require the protocol modification to enhance the network throughput.

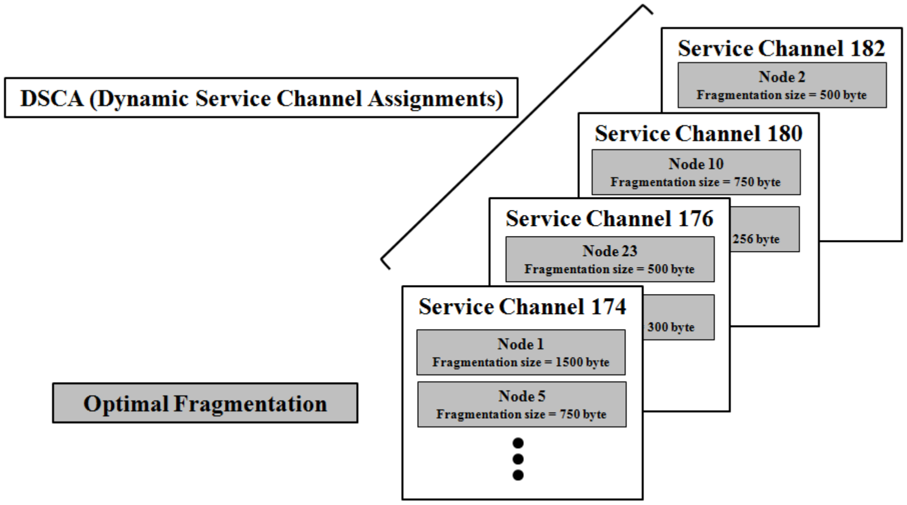

DSCA (Dynamic Service Channel Assignments)
Service Channel 182
Node 2
Fragmentation size = 500 byte
Service Channel 180
Node 10
Fragmentation size = 750 byte
256 byte
Service Channel 176
Node 23
Fragmentation size = 500 byte
300 byte
Service Channel 174
Node 1
Fragmentation size = 1500 byte
Node 5
Fragmentation size = 750 byte
Optimal Fragmentation

Figure 46: The contribution of this research.

The first technique is an optimal packet fragmentation with hidden stations. In real wireless environments, undesirable channel conditions can be generated by the interference from other devices, pathloss characteristic, fading, and collisions from both hidden nodes and contending nodes, and so forth. Since these problems occur simultaneously and they are correlated, they need to be modeled together rather than treated individually. Hence, Chapter 3 presents the detailed behavior of hidden nodes in noisy MANETs channels using the packet-fragmentation technique. The throughput of the IEEE 802.11 is fully modeled with hidden nodes by incorporating modified Markov-chain model with critical network parameters, such as BERs, number of users, packet length, and number of hidden nodes.

The simulation results using the fragmentation are compared to the results of RTS/CTS mechanisms. The optimal packet fragmentation not only reduces the packet-error rates, but also decreases the hidden-node collision probability. Therefore, when the channels suffer from hidden nodes and random-bit errors simultaneously, the optimal fragmentation could enhance network throughput more than RTS/CTS exchange. As a result, this technique utilizes the successful transmission time and enhances the entire network throughput.

Section 3.4 investigates the impact of both hidden nodes and random-bit errors (BERs) with respect to the fragment lengths through real-world experiments in noisy mobile ad-hoc networks (MANETs). Throughout real-world experiments under different weather condition, fading characteristic, and distances between nodes, we found that the hostile environment (low SNR and collisions from hidden nodes) deteriorates the network performance significantly. Moreover, as we observed in our experiment and other researchers indicated, the control frame exchanges of RTS/CTS signals not only waste channel resources, but also RTS/CTS signals are frequently lost due to the high BERs and collisions especially in noisy environments. We believe that this experiment result will provide a valuable real-world research results for the research communities to solve the hidden-node problem especially in noisy MANETs. Consequently, the novelty of this work lies on that the enhanced throughput can be achievable and implemented in real devices without deployment issues to solve both the hidden-node problem and random-bit errors simultaneously in noisy MANETs. In addition, Chapter 4 also validates the fragmentation technique incorporating the WAVE protocol in VANETs. Although the proposed technique can increase the network throughput under hostile channel conditions, we found that the short contention-window setting (high access categories) for the the priority service introduces severe collisions by the contending nodes. Therefore, we need to develop a technique to alleviate the collisions among high access categories as the second work of this thesis.

In Chapter 5, the dynamic service-channels allocation (DSCA) method is proposed to maximize throughput by dynamically assigning different service channels to the users. The solution for assigning multiple service-channels is based on the realistic assumptions in vehicular environments that include BERs, different access categories, and dense traffic conditions using single transceiver. DSCA is thoroughly analyzed based on Markov-chain model under the saturation conditions. To show the feasibility of DSCA, realistic parameters are used from the CISCO traffic statistics in NS-3 simulation. The average throughput is evaluated extensively under various channel conditions and vehicle densities. Moreover, both randomly generated and deterministically chosen traffic are studied in the simulation. As a result, the proposed DSCA enhances the average network throughput by 19% in deterministic access category scenario and by 22% in random access category scenario. DSCA also reduces the collision probability of high priority-access category packets, such as video and voice data, and thus, improves QoS of real-time traffic. The major contribution of this work is that DSCA can enhance throughput without the need for protocol modifications, multiple antennas, and the central coordination. DSCA does not sacrifice the performance of safety applications to solve multi-channel allocation problem in realistic VANETs environments. Moreover, inaccurate channel allocations will not degrade the performance due to the dynamic nature of selecting new optimal values in the DSCA algorithm.

For future work, a hidden-node detection algorithm in mobile ad-hoc networks will be investigated for the optimal fragmentation technique. One challenging problem in solving the hidden-node problem through our optimal fragmentation is that how we could know how many hidden terminals exist in the network and SNR values to incorporate the analytical results. Since this thesis more focuses on the accurate effects of both various BERs and different number of hidden nodes on the network throughput through real experiments than the fully automated implementation of our scheme, we calculate the optimal packet size in advance during the experiments. However, SNR values can be estimated accurately from [12], and the total number of nodes can be obtained by observing different MAC addresses. To get the number of hidden nodes, each sender could exchange the number of neighbor lists in the routing tables and could hear the acknowledgment packets from the receiver to other hidden nodes that are out of carrier sensing range of the sender. However, the detailed procedures for estimating the number of hidden nodes remain as a future work.

REFERENCES

[1] G. Bianchi, "Performance analysis of the ieee 802.11 distributed coordination function," *Selected Areas in Communications, IEEE Journal on*, vol. 18, pp. 535 –547, mar 2000.

[2] 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 *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 2, pp. 599 – 607 vol.2, 2002.

[3] X. Li and Q.-A. Zeng, "Influence of bit error rate on the performance of ieee 802.11 mac protocol," in *Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE*, pp. 367 –372, march 2007.

[4] F.-Y. Hung and I. Marsic, "Access delay analysis of ieee 802.11 dcf in the presence of hidden stations," in *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*, pp. 2541 –2545, nov. 2007.

[5] M. S. Gast, "802.11 wireless networks," *Book*, 2000.

[6] K. Xu, M. Gerla, and S. Bae, "How effective is the ieee 802.11 rts/cts handshake in ad hoc networks," in *Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE*, vol. 1, pp. 72 – 76 vol.1, nov. 2002.

[7] J. Sobrinho, R. de Haan, and J. Brazio, "Why rts-cts is not your ideal wireless lan multiple access protocol," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 1, pp. 81 – 87 Vol. 1, march 2005.

[8] S. Ray, J. Carruthers, and D. Starobinski, "Evaluation of the masked node problem in ad hoc wireless lans," *Mobile Computing, IEEE Transactions on*, vol. 4, pp. 430 – 442, sept.-oct. 2005.

[9] J. Yin, X. Wang, and D. Agrawal, "Optimal packet size in error-prone channel for ieee 802.11 distributed coordination function," in *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, vol. 3, pp. 1654 – 1659 Vol.3, march 2004.

[10] B.-S. Kim, Y. Fang, T. Wong, and Y. Kwon, "Throughput enhancement through dynamic fragmentation in wireless lans," *Vehicular Technology, IEEE Transactions on*, vol. 54, pp. 1415 – 1425, july 2005.

[11] J. Tourrilhes, "Fragment adaptive reduction: coping with various interferers in radio unlicensed bands," in *Communications, 2001. ICC 2001. IEEE International Conference on*, vol. 1, pp. 239 –244 vol.1, jun 2001.

[12] Y. Chang, C. Lee, and J. Copeland, "Goodput enhancement of vanets in noisy csma/ca channels," *Selected Areas in Communications, IEEE Journal on*, vol. 29, pp. 236 – 249, january 2011.

[13] A. Dubey, A. Jain, R. Upadhyay, and S. Charhate, "Performance evaluation of wireless network in presence of hidden node: A queuing theory approach," in *Modeling Simulation, 2008. AICMS 08. Second Asia International Conference on*, pp. 225 –229, may 2008.

[14] S. Khurana, A. Kahol, and A. Jayasumana, "Effect of hidden terminals on the performance of ieee 802.11 mac protocol," in *Local Computer Networks, 1998. LCN '98. Proceedings., 23rd Annual Conference on*, pp. 12 –20, Oct. 1998.

[15] S. Ray and D. Starobinski, “On false blocking in rts/cts-based multihop wireless networks,” *Vehicular Technology, IEEE Transactions on*, vol. 56, pp. 849 –862, march 2007.

[16] F. Tobagi and L. Kleinrock, “Packet switching in radio channels: Part ii–the hidden terminal problem in carrier sense multiple-access and the busy-tone solution,” *Communications, IEEE Transactions on*, vol. 23, pp. 1417 – 1433, dec 1975.

[17] A. Koubaa, R. Severino, M. Alves, and E. Tovar, “Improving quality-of-service in wireless sensor networks by mitigating "hidden-node collisions";,” *Industrial Informatics, IEEE Transactions on*, vol. 5, pp. 299 –313, Aug. 2009.

[18] Z. Haas and J. Deng, “Dual busy tone multiple access (dbtma)-a multiple access control scheme for ad hoc networks,” *Communications, IEEE Transactions on*, vol. 50, pp. 975 –985, jun 2002.

[19] A. Gummalla and J. Limb, “Wireless collision detect (wcd): multiple access with receiver initiated feedback and carrier detect signal,” in *Communications, 2000. ICC 2000. 2000 IEEE International Conference on*, vol. 1, pp. 397 –401 vol.1, 2000.

[20] B. Ji, “Asynchronous wireless collision detection with acknowledgement for wireless mesh networks,” in *Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd*, vol. 2, pp. 700 – 704, sept., 2005.

[21] J. Deng, B. Liang, and P. Varshney, “Tuning the carrier sensing range of ieee 802.11 mac,” in *Global Telecommunications Conference, 2004. GLOBECOM ’04. IEEE*, vol. 5, pp. 2987 – 2991 Vol.5, nov.-3 dec. 2004.

[22] H. Zhai and Y. Fang, “Physical carrier sensing and spatial reuse in multirate and multihop wireless ad hoc networks,” in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, pp. 1 –12, april 2006.

[23] S. Choobkar and R. Dilmaghani, “Enhancement of packetised-preamble based mac protocols: A solution to hidden-node problem in wsns,” in *Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium on*, pp. 192 –196, Sept. 2011.

[24] S. Park., Y. Chang, F. Khan, and J. Copeland, “Throughput enhancement of manets: Packet fragmentation with hidden stations and bers,” in *Consumer Communications and Networking Conference, 2012. CCNC 2012. 9th IEEE*, pp. 204–209, 2012.

[25] *OPNET simulator (http://www.opnet.com).*

[26] *Orinoco Proxim Gold Lancard (http://www.proxim.com).*

[27] P. Mahasukhon, M. Hempel, H. Sharif, T. Zhou, S. Ci, and H.-H. Chen, “Ber analysis of 802.11b networks under mobility,” pp. 4722 –4727, june 2007.

[28] “Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments,” *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008)*, pp. 1 –51, 15 2010.

[29] “Ieee standard for wireless access in vehicular environments (wave)–multi-channel operation,” *IEEE Std 1609.4-2010 (Revision of IEEE Std 1609.4-2006)*, pp. 1 –89, 7 2011.

[30] S. Grafling, P. Mahonen, and J. Riihijarvi, “Performance evaluation of ieee 1609 wave and ieee 802.11p for vehicular communications,” in *Ubiquitous and Future Networks (ICUFN), 2010 Second International Conference on*, pp. 344 –348, june 2010.

[31] C.-L. Huang and W. Liao, “Throughput and delay performance of ieee 802.11e enhanced distributed channel access (edca) under saturation condition,” *Wireless Communications, IEEE Transactions on*, vol. 6, pp. 136 –145, jan. 2007.

[32] *http://www.cisco.com.*

[33] F. Khan, Y. Chang, S. Park, and J. Copeland, “Handshaking vs. instant broadcast in vanet safety message routing,” in *Proceedings of IEEE PIMRC’11*, pp. 709–714, 2011.

[34] S.-I. Sou and O. Tonguz, “Enhancing vanet connectivity through roadside units on highways,” *Vehicular Technology, IEEE Transactions on*, vol. 60, pp. 3586 –3602, oct. 2011.

[35] C. Campolo, A. Vinel, A. Molinaro, and Y. Koucheryavy, “Modeling broadcasting in ieee 802.11p/wave vehicular networks,” *Communications Letters, IEEE*, vol. 15, pp. 199 –201, february 2011.

[36] N. Wisitpongphan, O. Tonguz, J. Parikh, P. Mudalige, F. Bai, and V. Sadekar, “Broadcast storm mitigation techniques in vehicular ad hoc networks,” *Wireless Communications, IEEE*, vol. 14, pp. 84 –94, december 2007.

[37] C. Sommer, O. Tonguz, and F. Dressler, “Traffic information systems: efficient message dissemination via adaptive beaconing,” *Communications Magazine, IEEE*, vol. 49, pp. 173 –179, may 2011.

[38] S. Eichler, “Performance evaluation of the ieee 802.11p wave communication standard,” in *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, pp. 2199 –2203, 30 2007-oct. 3 2007.

[39] H. Hartenstein and K. P.Laberteaux, “Vanet: Vehicular applications and internetworking technologies,” *Book*, 2010.

[40] S. eun Chung, J. Yoo, and C. kwon Kim, “A cognitive mac for vanet based on the wave systems,” in *Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on*, vol. 01, pp. 41 –46, feb. 2009.

[41] J. Jia, Q. Zhang, and X. Shen, “Hc-mac: A hardware-constrained cognitive mac for efficient spectrum management,” *Selected Areas in Communications, IEEE Journal on*, vol. 26, pp. 106 –117, jan. 2008.

[42] P. Fazio, F. De Rango, C. Sottile, and C. Calafate, “A new channel assignment scheme for interference-aware routing in vehicular networks,” in *Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd*, pp. 1 –5, may 2011.

[43] Y. Zang, L. Stibor, B. Walke, H.-J. Reumerman, and A. Barroso, “A novel mac protocol for throughput sensitive applications in vehicular environments,” in *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, pp. 2580 –2584, april 2007.

[44] N. Lu, Y. Ji, F. Liu, and X. Wang, “A dedicated multi-channel mac protocol design for vanet with adaptive broadcasting,” in *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*, pp. 1 –6, april 2010.

[45] R. Tomar and S. Verma, “Rsu centric channel allocation in vehicular ad-hoc networks,” in *Wireless Communication and Sensor Networks (WCSN), 2010 Sixth International Conference on*, pp. 1 –6, dec. 2010.

[46] K. Liu, J. Guo, N. Lu, and F. Liu, “Ramc: A rsu-assisted multi-channel coordination mac protocol for vanet,” in *GLOBECOM Workshops, 2009 IEEE*, pp. 1 –6, 30 2009-dec. 4 2009.

[47] R. Meireles, M. Boban, P. Steenkiste, O. Tonguz, and J. Barros, “Experimental study on the impact of vehicular obstructions in vanets,” in *Vehicular Networking Conference (VNC), 2010 IEEE*, pp. 338 –345, dec. 2010.

[48] Q. Li, J. Zhu, Q. Li, and C. Georghiades, “Efficient spatial covariance estimation for asynchronous co-channel interference suppression in mimo-ofdm systems,” *Wireless Communications, IEEE Transactions on*, vol. 7, pp. 4849 –4853, december 2008.

[49] “www.savarinetworks.com,” *Savarinetworks*.

[50] X. Xie, F. Wang, K. Li, P. Zhang, and H. Wang, “Improvement of multi-channel mac protocol for dense vanet with directional antennas,” in *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE*, pp. 1 –6, april 2009.

[51] M. Takata, M. Bandai, and T. Watanabe, “A mac protocol with directional antennas for deafness avoidance in ad hoc networks,” in *Global Telecommunications Conference, 2007. GLOBECOM ’07. IEEE*, pp. 620 –625, nov. 2007.