NTRCI

NATIONAL TRANSPORTATION RESEARCH CENTER, INCORPORATED
University Transportation Center

U29: Commercial Vehicle Secure Network for Safety and Mobility Applications Final Report

This project was funded by the NTRCI University Transportation Center under a grant from the U.S. Department of Transportation Research and Innovative Technology Administration (#DTRT-06-G-0043)

Alvin Lim, David Bevly

September 2011

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle **U29: Commercial Vehicle Secure Networks for Safety and Mobility Applications**		5. Report Date **September 2011** 6. Performing Organization Code
7. Author(s) **Alvin Lim, David Bevly**		8. Performing Organization Report No. **NTRCI-50-2011-24**
9. Performing Organization Name and Address **National Transportation Research Center, Inc.** **University Transportation Center** **9125 Cross Park Drive** **Suite 150** **Knoxville, TN 37923**		10. Work Unit No. (TRAIS) 11. Contract or Grant No. **RITA Grant – DTRT06G-0043**
12. Sponsoring Agency Name and Address **U.S. Department of Transportation** **Research and Innovative Technology Administration** **1200 New Jersey Avenue, SE** **Washington, DC 20590**		13. Type of Report and Period Covered **Final Report** **January 2011 – September 2011** 14. Sponsoring Agency Code
15. Supplementary Notes **Special thanks to: Auburn University and Bishop Consulting**		

16. Abstract

The main objective of this project is to develop a secure, reliable, high throughput and integrated wireless network for Vehicle-To-Vehicle (V2V), Vehicle-To-Infrastructure (V2I) and intra-vehicle communications. Novel techniques and communication protocols were developed to ensure that safety messages are transmitted reliably, securely and efficiently.

The secure network protocols using IEEE 802.11i authentication and anti-jamming dynamic channel hopping protocol were implemented and the results show an improved performance. These security mechanisms will avoid not only attackers from disrupting critical vehicle communication but also enable high connectivity and performance even in the presence of benign transmissions that may interference with the vehicle network transmissions. The adaptive multi-hop routing ensures end-to-end connectivity by considering the connectivity of each wireless links. These protocols demonstrated how to transmit high priority urgent messages reliably. The rate adaptation algorithm was implemented and the results show improved performance since it avoids packet collisions and tolerate channel fading in the harsh vehicle environment. The precise vehicle positioning technique is integrated with the wireless vehicle networks that provide reliable, secure and high throughput transmissions of GPS messages.

The results of our studies on the integrated wireless vehicle networks for V2V, V2I and intra-vehicle networks show that the integrated network can satisfy the security, reliability and throughput performance requirements of Electronic Stability Control (ESC) systems and other connected vehicle safety applications. The demonstration of the intra-vehicle wireless networks on the commercial tractor trailers at the National Center for Asphalt Technology (NCAT) test track for supporting ESC systems showed that this is feasible in real-world vehicle networks under normal operating conditions.

17. Key Word	18. Distribution Statement
Secure, reliable, and high throughput wireless network; vehicle-to-vehicle, vehicle-to-infrastructure communications; authentication; dynamic channel hopping; rate adaptation algorithm; precise vehicle positioning	**No restrictions**

19. Security Class if. (of this report)	20. Security Class if. (of this page)	21. No. of Pages	22. Price
Unclassified	**Unclassified**	**86**	

This page intentionally left blank.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Definition
AES	Advanced Encryption Standard
AES-CCMP	Advanced Encryption Standard - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
AP	Access Point
APM	Antenna Polarization Mismatch
Auburn	Auburn University
CAN	Controller Area Network
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CN	Cluster Head Node
DCA	Direct Communication Area
DD	Double Differences
DGPS	Differential Global Positioning System
DoS	Denial of Service
DOT	U.S. Department of Transportation
DRTK	Dynamic Base Real-Time Kinematic
DSRC	Dedicated Short-Range Communication
EAP	Extensible Authentication Protocol
ECA	Extended Communication Area
ESC	Electronic Stability Control. In this report, ESC is used as a generic term for any electronic system that automatically applies brakes on the tractor or semitrailer to enhance the stability of the vehicle in any way.
FRRA	Fast Recovery Rate Adaptation
GPS	Global Positioning System
GTK	Group Transient Key
IEEE	Institute of Electrical and Electronic Engineers
IEF	Initial Electing Factor
IN	Infrastructure Nodes
IP	Internet Protocol
ISO	International Organization for Standards
LCV	Longer Combination Vehicle
MAC	Media Access Control
MCS	Modulation Coding Scheme
MIMO	Multiple-input, Multiple-output
MRR	Multi-rate Retry
MSK	Master Session Key
NCAT	National Center for Asphalt Technology
NHTSA	National Highway Traffic Safety Administration
NTRCI	National Transportation Research Center, Inc.

Abbreviation	Definition
PHY	Physical (layer)
PMK	Pairwise Master Key
PSK	Pre-shared Key
PTK	Pairwise Transient Key
RITA	Research and Innovative Technology Administration
RPV	Relative Position Vector
RSN	Robust Security Network
RSNA	Robust Security Network Associations
RTK	Real-Time Kinematic
SD	Single Differencing
SMM	Spatial Multiplexing Malfunction
SNR	Signal to Noise Ratio
STBC	Space-Time Block Code
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

Units of Measure

Unit Abbreviation	Meaning
B	Bytes
b	Bits
ft	Feet
GB	Gigabyte
GHz	Gigahertz
Hz	Hertz
kbps	Kilobits per second
km	Kilometers
km/h	Kilometers per hour
m	Meter
Mbps	Megabits per second
MHz	Megahertz
mi	Mile
min	Minutes
mph	Miles per hour
ms	Milliseconds
µs	Microseconds
mW	Milliwatt
s	Seconds
W	Watt

This page intentionally left blank.

Executive Summary

The main objective of this project was to develop a secure, reliable, high throughput and integrated wireless network for Vehicle-To-Vehicle (V2V), Vehicle-To-Infrastructure (V2I) and intra-vehicle communications. Novel techniques and communication protocols were developed to ensure that safety messages are transmitted reliably, securely and efficiently. The integrated wireless network allows warning messages of tractor-trailer instability to be transmitted from a trailer to the electronic stability control (ESC) system at the tractor that then responds with control messages to the brake actuators to stabilize the vehicle. The integrated networks also allow warning messages to be transmitted between neighboring vehicles to alert the drivers to avoid potential collisions. Five tasks were completed to implement the integrated wireless network.

The first task developed the framework and core integrated vehicle architecture for three types of wireless communication ─ V2V, V2I and intra-vehicle networking ─ based on dynamic clustering for dynamic channel allocation and security management. The second task developed secure wireless vehicle networks to ensure messages are transmitted securely by implementing the Institute of Electrical and Electronic Engineers (IEEE) standard IEEE 802.11i authentication and key management security protocols as well as other anti-jamming countermeasures, such as dynamic channel hopping. The third task developed algorithms for improving the reliability of wireless vehicle networks to ensure that vehicle ESC systems and other safety applications are able to transmit critical sensors, actuator and warning messages reliably. The fourth task developed techniques for improving the throughput to ensure that all critical messages, such as sensor, actuator control and safety alert messages can be transmitted at the highest possible transmission rate. The fifth task developed techniques for precise vehicle positioning using multiple Global Positioning System (GPS) units at the tractor and trailer in order to compute accurate trailer position relative to the tractor.

Background

Commercial vehicle wireless networks are beneficial for supporting many safety and mobility applications. Integrated network supports three forms of vehicle wireless networks: Intra-vehicle wireless networks, V2V networks, and V2I networks. Each of these forms of wireless vehicle networks provides a wide range of benefits in different scenarios. Intra-vehicle wireless communication provides many benefits in supporting vehicle stability control systems where the sensor and actuator control data are transmitted wirelessly between the tractor and trailers. For instance, trailers and tractors may be interchanged easily without the need to plug in the connectors for the sensor and actuator signal cable. The signals will be dynamically transmitted through the wireless channels at a high data rate and reliability. V2V communication can provide benefits in sending critical safety information from one vehicle to another. For instance, a tractor trailer that has detected its long combination instability problem can send warning messages to the neighboring vehicles. V2I wireless networks can provide benefits in communicating

important road, traffic, terrain, or weather information. For instance, a sharply curved road may have a roadside wireless infrastructure node that constantly sends wireless messages to vehicles about the sharpness of the curve in the road.

Brief Overview

The framework and core integrated vehicle network architecture is based on dynamic clustering for dynamic channel allocation and security management. The common framework enabled integration of network protocols, such as security, reliability, and high throughput protocols. The secure vehicle network implemented IEEE 802.11i authentication and key management security protocols as well as other anti-jamming countermeasures, such as dynamic channel hopping. Various techniques for improving wireless network reliability were developed, including optimizing antenna orientation, multi-hop packet forwarding and efficient broadcast mechanisms. To ensure that these dynamic signals are communicated at a high data rate and reliability, a rate adaptation algorithm that can accurately distinguish channel fading from data packet collisions was developed. For precise vehicle positioning, data collections and analysis were used to provide understanding of the accuracy and reliability of the GPS based relative positioning in the tractor-trailer.

Research Strategy

The secure network protocols using IEEE 802.11i authentication and anti-jamming dynamic channel hopping protocol were implemented and the results showed an improved performance. These security mechanisms will avoid not only attackers from disrupting critical vehicle communication but also enable high connectivity and performance even in the presence of benign transmissions that may cause interference with the vehicle network transmissions. The adaptive multi-hop routing ensures end-to-end connectivity by considering the connectivity of each wireless link. These protocols demonstrated how to transmit high priority urgent messages reliably. The rate adaptation algorithm was implemented and the results showed improved performance since it avoids packet collisions and tolerates channel fading in the harsh vehicle environment. The precise vehicle positioning technique is integrated with the wireless vehicle networks that provide reliable, secure and high throughput transmissions of GPS messages.

Conclusion

This research work on developing novel wireless vehicle network protocols and techniques will move commercial connected vehicle research closer to deployment since these communication protocols and algorithms can ensure that safety messages are transmitted reliably, securely and efficiently even in the harsh vehicle wireless environments. Empirical tests of the wireless communication in actual commercial tractor semi-trailers show that wireless vehicle network can improve performance and support various safety and ESC systems. Despite the harsh wireless vehicle environments, the reliability and throughput results of these wireless techniques show that they can meet the reliability, security and throughput requirements of the ESC system.

Future Program Efforts

In order for these novel wireless vehicle network protocols and techniques to be deployed and support commercial connected vehicle research there is a further need for tests on the performance, reliability, security and feasibility of practical wireless devices that can be installed on the commercial tractor-trailer. The size and cost of the wireless devices that will still meet the throughput and reliability requirements will continue to be reduced. More tests will need to be conducted to evaluate the performance and reliability of the protocols under more hazardous wireless conditions, such as heavy rain, fog or snow. Wireless protocols will be designed specifically to overcome these adverse weather conditions.

For the integrated wireless vehicle network to be deployed in real commercial vehicles on the actual road and in highway conditions, the current protocols need more improvements to provide higher reliability and throughput. More efficient techniques should be investigated in dynamic clustering for dynamic channel allocation and security management. The security of wireless vehicle networks will be improved to avoid potential security loop-holes and problems in the implementation of IEEE 802.11i authentication and key management. To avoid jamming, better countermeasure techniques will be developed that will also provide high throughput and reliability. More advanced protocols and techniques will be developed to improve wireless network reliability, which could be based on variations of multi-hop packet forwarding and efficient broadcast mechanisms. Additionally, further development on rate adaptation algorithms will improve accuracy in distinguishing channel fading from data packet collisions. Precise vehicle positioning may also be improved using the current data collections and analysis to design more accurate and reliable GPS based relative positioning in the tractor-trailer.

This page intentionally left blank.

Chapter 1 – Introduction and Background

A team at Auburn University led by the National Transportation Research Center, Inc., (NTRCI) worked on developing an integrated secure, reliable and high-performance wireless vehicle network for supporting commercial vehicle safety and mobility applications. The algorithms and protocols are designed and implemented in software and deployed in hardware for experimentations, demonstration and performance evaluation.

The feasibility of using a wireless intra-vehicle network has been investigated in a concurrent project for supporting an electronic stability control (ESC) system that improves the roll and yaw stability of combination heavy duty commercial trucks (Pape et al., 2011). The wireless intra-vehicle network provides adequate capability to meet the wireless networking requirements for sensor and control data transmission of the sensor and control hardware utilized in the stability algorithms. The feasibility of using wireless Vehicle-To-Vehicle (V2V) and Vehicle-To-Infrastructure (V2I) networks were also investigated for disseminating warning, alerts and informational messages.

1.1 Background

Wireless vehicle networks must provide reliability, security and high throughput to support commercial vehicle safety and mobility applications. Because of the harsh wireless environment in which vehicle networks operate, the reliability, security and performance may not necessarily meet the transmission requirements for various safety and mobility applications. New techniques, algorithms and protocols must be developed to ensure that critical wireless communications are reliable, secure and meet the throughput requirements of these applications. These new techniques will benefit the U.S. Department of Transportation (US DOT) Connected Vehicles Research Program and offers the potential to enhance wireless communication and connectivity. The purpose of this project was to develop an integrated secure, reliable and high-performance wireless vehicle network for supporting commercial vehicle safety and mobility applications. The algorithms and protocols were designed for supporting V2V, V2I and intra-vehicle wireless network. In intra-vehicle networks, sensor and control data can be transmitted wirelessly between semitrailers and a tractor to help a driver maintain control of a combination unit vehicle and communicate safety information to neighboring vehicles. V2V and V2I wireless networks are designed to enable warning, alert and informational messages to be exchanged reliably and securely.

1.2 Motivation for Commercial Vehicle Wireless Networks

Commercial vehicle wireless networks are beneficial for supporting many safety and mobility applications. There are three forms of vehicle wireless networks: Intra-vehicle wireless networks, V2V networks, and V2I networks. Each of these forms of wireless vehicle networks provides a wide range of benefits in different scenarios.

Intra-vehicle wireless communication provides many benefits in supporting vehicle stability control systems where the sensor and actuator control data are transmitted wirelessly between the tractor and trailers. First, trailers and tractors may be interchanged easily without the need to plug in the connectors for the sensor and actuator signal cable. The signals will be dynamically transmitted through the wireless channels at a high data rate and reliability. Second, the wireless channel enables transmission of different types of signals typically sent through different types of cables, such as the Controller Area Network (CAN) data bus, serial cable, and Ethernet. With this capability, commercial vehicle drivers need not have to deal with the different types of connectors. Third, wireless transmission can enable the different types of signals to be integrated into a single standard for wireless sensor data and actuator transmission. This will simplify the development of new sensors and actuators, which may eliminate the need to deal with different types of sensor and actuator data bus protocols.

V2V communication can provide benefits in sending critical safety information from one vehicle to another. For instance, a tractor trailer that has detected its long combination instability problem or potential collision course with another vehicle can send warning or alert messages to the neighboring vehicles. The warning messages could also contain critical vehicle dynamics information, such as position, velocity, acceleration and lateral acceleration. This critical real-time information can be used by the neighboring vehicles to compute their potential involvement in any predicted collision or determine their appropriate corrective actions in the adaptive cruise control system to apply to their actuators, such as brake and steering control.

V2Iwireless networks can provide benefits in communicating important road, traffic, terrain, or weather information. For instance, a sharply curved road may have a roadside wireless infrastructure node that constantly sends wireless messages to vehicles about the sharpness of the curve in the road. The commercial vehicle will receive the sharpness information and depending on their tractor-trailer combination characteristics, it can compute the maximum speed that it can safely travel around the curved road. If the actual speed of the commercial vehicle is above this maximum safe speed, a red alert sign will flash the driver to slow down. Alert messages could also be sent to other neighboring vehicles to warn them of impending stability problems.

1.3 Challenging Problems of Commercial Vehicle Secure Wireless Networks

In the actual deployment of commercial vehicle wireless networks for supporting V2V, V2I and intra-vehicle communications, there are many challenging problems that must be addressed. Because of the high mobility of vehicles, connectivity must be ensured and channel must be managed efficiently for V2V, V2I and intra-vehicle communications. Furthermore, these problems are aggravated by the harsh wireless conditions in which these networks operate where wireless transmission may deteriorate due to many reasons, including channel fading, collisions, occlusion, congestion, and interference. Even in intra-vehicle networks which are relatively more static than V2V and V2I networks, these harsh wireless conditions persist and cause degradation in wireless transmissions and connectivity.

Because of the high mobility of vehicles, an important issue is the time for dynamic association among the vehicle wireless devices for the purpose of managing channels and exchanges of protocol packets before communication of data packets is enabled among the vehicles. For V2I communication, the problems are simpler because the fixed Infrastructure Nodes (IN) can manage the channel and data exchanges. Even then, the high mobility of vehicles makes it necessary for the vehicles to associate with the IN quickly to enable channel allocation and protocols for data packet exchanges without collision. For V2V communication, these problems are particularly difficult because there must be a node called the Cluster Head Node (CN) that coordinates the channel allocation which must be elected from a dynamically changing cluster of vehicle nodes. Even for intra-vehicle networks where there may be a static CN, there are problems of dynamic selection of the best channel for the wireless nodes in the semitrailers to communicate with the tractor due to problems of jamming and interference.

In addition to the channel management and protocols to enable interference-free communication, poor wireless channel quality may cause potential problems for commercial vehicle wireless networks. This is particularly more evident since wireless technologies have proliferated, greatly increasing the number of applications that use wireless access by mobile/portable devices. The increase in the amount of wireless traffic leads to poor channel quality. Channels can deteriorate due to any of six main reasons:

1. Signal fading caused by signal propagation loss between two associated stations and effects of multi-paths
2. Collision caused by simultaneous transmissions from different stations
3. Interference from nearby unrelated signals or jammers
4. Congestion in the network that may cause packet loss
5. Occlusion due to objects that obstruct radio propagation
6. Antenna placement and orientation as well as vehicle movement that may cause deterioration in wireless reception

Since these causes cannot be eliminated due to the unstable nature of the wireless medium, appropriate adaptive protocols must be used to address each of these sources of wireless channel degradation more accurately.

To improve the performance of wireless vehicle networks, an understanding of the characteristics of outdoor wireless transmission environments as well as the effects of mobility is needed. First, the signal propagation delay increases in outdoor wireless networks due to larger transmission distance compared to indoor wireless networks, which in turn may affect the performance of the Media Access Control (MAC) protocol. Second, the outdoor wireless

environment has increased delay spread that causes inter-symbol interference. Third, Doppler effects due to mobility may require sophisticated channel estimation.

1.4 Project Team

At Auburn University, the Pervasive Computing and Wireless Networking Laboratory, the Global Positioning System (GPS) and Vehicle Dynamics Laboratory and Auburn University National Center for Asphalt Technology (NCAT) had leading roles in the technical work of this project. Bishop Consulting provides consultation and advice on some of the aspects of this project. The following are more complete descriptions of each and its role.

1.4.1 Auburn University Pervasive Computing and Wireless Networking Laboratory

Dr. Alvin Lim directs the Pervasive Computing and Wireless Networking Laboratory and had primary responsibility for the investigation of secure and robust wireless communication between units of a combination vehicle, between vehicles and between vehicle and infrastructure wireless devices.

1.4.2 Auburn University GPS and Vehicle Dynamics Laboratory

Dr. David Bevly directs the GPS and Vehicle Dynamics Laboratory and had the responsibility for the investigation of precise vehicle positioning, where data collected from multiple GPS receivers mounted on a tractor-trailer provide the data that can be analyzed to compute the trailers precise position.

1.4.3 Auburn University National Center for Asphalt Technology (NCAT)

The NCAT at Auburn University provides supports for the test track, long combination tractor trailers, drivers and the test facilities for conducting experiments on wireless vehicle networks and data collection.

1.4.4 Bishop Consulting

Richard Bishop of Bishop Consulting provides advice on current research on intelligent vehicles and wireless vehicle communication in other federal government agencies, vehicle manufacturers and research laboratories.

1.5 Project Description

The main objective of this project was to develop a secure, reliable, high throughput and integrated wireless network for V2V, V2I and intra-vehicle communications. This work will move commercial connected vehicle research closer to deployment by developing communication protocols and algorithms which can ensure that safety messages are transmitted reliably, securely and efficiently. For instance, warning messages of tractor-trailer instability over a sharply curved road could be transmitted from a trailer to the driver in the tractor or to the

ESC system to send control messages to the brake actuators to stabilize the commercial vehicle. These instability warning messages and other imminent collision warnings could also be transmitted to other neighboring vehicles to alert the drivers to avoid potential collisions.

The first task was to develop the framework and core integrated vehicle network architecture for three types of wireless communication: V2V, V2I and intra-vehicle networking. This core architecture is based on dynamic clustering for dynamic channel allocation and security management. The common framework is designed to enable various types of other network protocols to be developed and integrated into the vehicle network. These network protocols, including security, reliability, and high throughput protocols, are designed for vehicle communication as described below.

The second task was to develop secure wireless vehicle networks to ensure messages are transmitted securely in V2V, V2I and intra-vehicle communications. The main focus was on implementation of the Institute of Electrical and Electronic Engineers (IEEE) standard IEEE 802.11i authentication and key management security protocols as well as other anti-jamming countermeasures, such as dynamic channel hopping. These security mechanisms will avoid not only attackers from disrupting critical vehicle communication but also enable high connectivity and performance even in the presence of benign transmissions that may interfere with the vehicle network transmissions.

The third task was to improve the reliability of wireless vehicle networks since vehicle ESC systems and other safety applications require that critical sensors, actuator and warning messages must be transmitted reliably. Various techniques were investigated for improving wireless network reliability, including optimizing antenna orientation, multi-hop packet forwarding and efficient broadcast mechanisms. The adaptive multi-hop routing ensures end-to-end connectivity by considering the connectivity of each wireless links. These protocols demonstrated how to transmit high priority urgent messages reliably.

The fourth task was to improve the throughput of wireless packet transmission to ensure that all critical messages, such as sensor, actuator control and safety alert messages can be transmitted at the highest possible transmission rate in order for the ESC application to function properly and for the safety applications to respond rapidly to alert messages. To ensure that these dynamic signals are communicated at a high data rate and reliability, a rate adaptation algorithm was developed that can accurately distinguish channel fading from data packet collisions. This adaptive capability was necessary to avoid packet collisions and tolerate channel fading in the harsh vehicle environment.

The fifth task was to develop techniques for precise vehicle positioning using multiple GPS units at the tractor and trailer in order to compute accurate trailer position relative to the tractor. Data collections and analysis in this investigation provided a better understanding of the accuracy and reliability of the GPS based relative positioning in the tractor-trailer. This precise vehicle

positioning technique is integrated with the wireless vehicle networks that provide reliable, secure and high throughput transmissions of GPS messages.

Chapter 2 – Literature Review

2.1 Wireless Communication Protocols

Wireless vehicle networks may be built using different wireless protocols, such as IEEE 802.11a/b/g/n, Dedicated Short-Range Communication (DSRC) (IEEE 802.11p), WiMAX, ZigBee, among others. To select the best wireless protocol for V2V, V2I, and intra-vehicle wireless networks we conducted some performance and usability studies to compare these wireless protocols, particularly in the commercial vehicle environments. Some of these studies are based on qualitative analyses, while others are based on performance measurements of the actual wireless transmission using performance tools, such as a product named "Iperf."

2.1.1 IEEE 802.11a/b/g/n ("Wi-Fi")

The IEEE 802.11 standard consists of a family of protocols. In this particular category a group of related protocols that are commercially available are considered (e.g., IEEE 802.11a/b/g/n protocols, which are generally known as Wi-Fi networks). Versions a, b, and g are prior versions; the current version, IEEE 802.11n, is the highest performing. There are many benefits in using IEEE 802.11n because of its many advanced features, including Multiple-Input, Multiple-Output (MIMO), spatial multiplexing, Modulation and Coding Scheme (MCS), Space-Time Block Code (STBC), channel bonding, and frame aggregation. These features enable IEEE 802.11n to transmit at a rate of more than 100 Mbps (with two antennas) with reasonably low packet loss rate. This is the main reason why IEEE 802.11n was selected over the other protocols for the prototype intra-vehicle wireless network.

IEEE 802.11n operates in two ISM bands, either in the 83.5 MHz bandwidth of the 2.4 GHz band or at the 125 MHz bandwidth of the 5.8 GHz band. The bit rate of the wireless link depends on the size of the spectrum. However, the bit rate limitation can be overcome using MIMO antenna technology, which uses several antennas to create multiple streams of data. Depending on the number of antennas, IEEE 802.11n can achieve a bit rate of up to 300 Mbps, when configured with three antennas. The transmission range of IEEE 802.11n in ideal conditions is about 53.3 m (175 ft.) (in the 2.4 GHz frequency block), longer than a turnpike double with two 14.6 m (48-ft.) trailers (Ervin et al., 1984).

However, in vehicle wireless networking environments, there are some pitfalls in the use of IEEE 802.11n (as well as the other wireless protocols described below), which could affect the performance and reliability of intra-vehicular wireless communication. The performance could degrade due to the harsh operating environment, including mobility, congestion, collision, interference, jamming, vibration, and Antenna Polarization Mismatch (APM). This research work shows how performance may be improved using techniques for overcoming some of these problems. Although the performance is done specifically using IEEE 802.11n, the techniques may also be extended to other protocols, for example, DSRC.

2.1.2 DSRC (IEEE 802.11p)

The main advantage of using DSRC is that it uses the 5.9 GHz band that is specially allocated for vehicle networks, whereas IEEE 802.11n is used for a very wide range of wireless applications. However, the main disadvantage is that it does not include many of the advanced features of IEE 802.11n, and thus gives lower performance and reliability.

The U.S. Federal Communications Commission (FCC) allocated the 75 MHz bandwidth of the 5.9 GHz band for V2V and V2I wireless communication in 1999 (Cheng et al., 2007). The commission then established the service and license rules for DSRC service, which operates on the 5.850 to 5.925 GHz band for public safety and private applications in vehicular networks. In 2001, ASTM International selected IEEE 802.11a as the underlying radio technology of DSRC's Physical (PHY) layer (ASTM, 2003). In 2004, the IEEE started the work on the 802.11p amendment and Wireless Access in Vehicular Environments (WAVE) standards based on the ASTM standard. The transmission range of DSRC is about 1000m.

DSRC supports both safety and commercial non-safety applications by providing separate channels. The 75 MHz licensed spectrum is divided into 7 different channels with 10 MHz channel bandwidth each. Both safety and non-safety applications can co-exist through a periodic Time Division Multiplexing (TDM) scheme. TDM in the application level is achieved using time synchronization between the communicating units, for example, using Universal Coordinated Time, as proposed in the IEEE communication standards in development for the DSRC band.

2.1.3 WiMAX

WiMAX is designed for wireless metropolitan-area networks. It provides a service range of up to 50 km (31 mi), shared data rates of up to 70 Mbps, and a peak data rate of up to 268 Mbps. The WiMAX standard IEEE 802.16a supports non-line-of-sight transmission in the range between the 2 GHz and the 22 GHz bands. IEEE 802.16e-2005 supports mobility, but has a peak downstream data rate of 12 Mbps and an upstream data rate of 2 Mbps to 5 Mbps. Its range is less than 50 km. WiMAX operates on both the unlicensed frequencies of the 2.4 GHz and 5.8 GHz bands and the licensed frequencies of the 2.5 GHz and 3.5 GHz bands. For industrial purposes, the licensed spectrum is used. Mainly because of the licensed frequencies and the low throughput, WiMAX is not considered for wireless vehicle communication.

2.1.4 Other Wireless Communication Protocols

There are other low-powered wireless protocols, such as ZigBee (IEEE 802.15.4) and Bluetooth (IEEE 802.15.1). These wireless protocols are designed for wireless personal area networks (WPANs) with smaller coverage area and lower power consumption. ZigBee operates at the frequency spectrum of 902 to 928 MHz and 2.4 GHz, whereas Bluetooth operates at 2.4 GHz. The transmission range of ZigBee is 100 m, while that of Bluetooth is only 10 m. On the other hand, the data rate of ZigBee is only 20 to 250 kbps, while that of Bluetooth is 1 Mbps. Because

of their low data rates and transmission range, these protocols are not considered for vehicle networks.

2.2 Secure Vehicle Wireless Networks

Wireless networks have been prone to many types of attacks, Denial of Service (DoS) attacks being the most harmful ones. The DoS attack “jamming” can cause significant performance degradation of a network by interference. Attackers can jam the network using various types of jammers. The resulting non-functionality of the network combined with the ease of launching a jamming attack makes it necessary to develop reliable systems to act against these types of attack. There are two parts of an anti-jamming system; jamming detection and countermeasure. Over the last few years a good amount of work has been done on developing such systems.

2.2.1 Jamming and Jammers

Jamming is the activity of blocking the communication channel by achieving one of the following goals: consumption of computational resources; disruption of computational information, state information, or physical network components; or obstructing the communication media between the intended users and the victim (Xu et al., 2005). Various types of jammers have been used by several researchers. Jammers can be elementary or advanced; elementary jammers can be classified as proactive or reactive while the advanced ones can be either function-specific or smart-hybrid jammers.

Elementary proactive jammers can be constant, deceptive, or random (Xu et al., 2005). Their main aim is to keep the channel busy so that the legitimate nodes are not able to access it. On the other hand, the reactive jammers disrupt packets sent by one legitimate node to another (Pelechrinis et al., 2011). Advanced function-specific jammers are the ones having a predefined function like follow-on (Mpitziopoulos, 2007), channel hopping (Alnifie et al., 2010) and pulsed-noise (Muraleedharan et al., 2006) jammers. Smart-hybrid jammers are control-channel jammers (Lazos et al., 2009), implicit jammers (Broustis et al., 2009) and flow jammers (Tague et al., 2008). They have power efficiency and effective jamming nature, hence smart.

2.2.2 Jamming Detection and Resilience

Due to the importance of effective jamming detection, many techniques have been proposed. Typical jammed network results from two conditions; either the attacker makes the channel unavailable for the sender to access or it corrupts the packets sent by the sender. The former attack can be detected at the sender end using utility threshold and carrier sensing parameters while the latter needs to be detected at the receiver end with the help of packet delivery ratio or Signal to Noise Ratio (SNR). Also, it is required to look into the details of methods which can provide resilience for them.

Authors of Wood et al. (2003) have given a detection and mitigation method which maps out the jammed area in wireless sensor networks and routes packets around the affected region. While an

evolutionary algorithm to detect jamming at the PHY layer has been proposed in Muraleedharan (2006), and redirects messages to an appropriate destination node. Authors of Jain et al. (2009) propose a hybrid anti-jamming system by combining 3 defense techniques: base station replication, base station evasion and multipath routing between base stations. On the other hand, an effective jamming detection using either location or signal strength consistency check along with packet delivery ratio determination is proposed in Xu et al. (2005). A centralized jamming detection system in Misra et al. (2010) computes the jamming index using the SNR and packet dropped per terminal (PDPT) values. Channel surfing (or channel hopping) is another technique proposed in Xu et al. (2006).

2.3 Reliability in Wireless Vehicle Networks

Complete details of IEEE 802.11n technology are discussed in Paul and Ogunfunmi (2008) where the evolution of the IEEE 802.11n amendment is described following the discussion on the previous generation Wireless Local Area Network (WLAN) devices (IEEE 802.11a/b/g). The key technique in IEEE 802.11n is the MIMO technology which forms the foundation of high performance by transmitting and receiving data from multiple antennas. To understand the performance of MIMO, Paul and Ogunfunmi (2009) investigate IEEE 802.11n PHY layer, and Medvedev et al. (2006) discuss the complexity of various MIMO receiver structures for IEEE 802.11n WLANs. Moreover, the performance and enhancement of the MAC layer of IEEE 802.11n are investigated in Abraham et al. (2005); Wang and Wei (2009); Xiao (2005).

All the above-mentioned papers are either based on mathematical analysis or simulations, so the evaluation results cannot be used directly on analyzing the reliability of actual IEEE 802.11n networks. On the other hand, Fiehe et al. (2010) study the performance of IEEE 802.11n using extensive measurement campaigns carried out in both interference-controlled and typical office environments. They discover that in a typical office environment significant performance improvement can be expected in IEEE 802.11n but theoretically achievable bit rates cannot be reached. So far, there is no work about the empirical study of applying IEEE 802.11n in an outdoor environment, such as vehicular networks.

As discussed in Stallings (2004), the WiFi technology including IEEE 802.11a/b/g/n is originally designed for indoor use. Due to dynamic communication environments of outdoor WiFi networks, as described by Paul et al. (2011), it is difficult to achieve reliable performances. Particularly, Jarupan and Ekici (2011) discover the complexity and instability of communications in outdoor vehicular networks. To address these issues, much work has been done on applying WiFi technology to vehicular networks such as Bychkovsky et al. (2006); Mahajan et al. (2007); Eriksson et al. (2008); Balasubramanian et al. (2008). Bychkovsky et al. (2006) conducted a measurement study with over 290 “drive hours” over a few cars under typical driving conditions, and they conclude that WiFi networks cannot provide reliable networking for vehicular network but can support only some delay-tolerant applications. The high mobility of vehicles led Mahajan et al. (2007) to investigate the connection times between vehicles and roadside Access Points

(AP). They concluded that regular periods of disconnection occur as vehicles move through areas poorly covered by the APs. In the Cabernet project, Eriksson et al. (2008) studied how to deliver vehicular content using WiFi, and they concluded that only non-interactive vehicular applications can be supported by WiFi. In other works, it is impossible to use existing AP infrastructures to build reliable vehicular networks. To address this issue, Balasubramanian et al. (2008) proposed a new network access method called ViFi which uses a decentralized and lightweight probabilistic algorithm for coordination between participating base stations to minimize disruptions and support interactive applications for vehicles. Most previous work of WiFi vehicular networks focus on V2I communications where vehicles are considered the wireless clients connecting to roadside APs to achieve network access. There is only limited work that studies V2V communications. For example, Jerbi et al. (2007) confirmed the feasibility of using ad hoc networks to extend the transmission range of the infrastructure and reduce the connection time for moving cars in vehicular networks.

In summary, most experimental studies on applying WiFi (IEEE 802.11a/b/g) technology to vehicular networks focused on building fast connections between cars and roadside APs to achieve V2I communications. On the other hand, performance evaluations of IEEE 802.11n are conducted either on MAC or PHY layers for indoor environments. This study is the first to empirically investigate the network reliability of inter-vehicle and intra-vehicle communications in IEEE 802.11n based vehicular networks.

This page intentionally left blank.

Chapter 3 – Integrated Architecture for Vehicle Networks

3.1 Overview of Architecture for Vehicle Networks

The integrated architecture for wireless vehicle networks combines three types of wireless vehicular communications in a network: V2V, V2I and Intra-vehicle communications. V2I communication will be dedicated for huge-volume communications, network authentication, and emergency message propagation. Regular data transmission will be forwarded through V2I communication where IN are available and through V2V nodes whenever they are available. Emergency packets may be delivered through multi-hop V2V communication if there is not roadside infrastructure available or the network traffic loads on them are too heavy to meet message delivery requirements. Intra-vehicle communication is also important for a driver, particularly semi-truck and heavy vehicles, to monitor its vehicle's real-time conditions, such as stability and lateral acceleration.

To integrate these different communications into one network system, a cluster based vehicular network architecture was developed. Each cluster has at least one CN (CN) and a set of members. Generally, the members of one cluster have some common characteristics such as contiguous velocities or coordinates. Cluster based solutions represent a viable approach for propagating messages among vehicles. In addition, a CN will serve as a dynamic channel hopping coordinator for its cluster members so that different channels are allocated to different communication links to avoid potential co-channel interference.

As shown in Figure 3-1, depending on whether there is a nearby infrastructure wireless node available, the entire network area is (geographically) divided into two parts: the Direct Communication Area (DCA) and Extended Communication Area (ECA). A DCA is an area that is within the coverage area of an infrastructure node. If a vehicle moves into a DCA, the channel allocation will be performed by the roadside infrastructure and then a V2I communication is initiated. An ECA is a one-hop segment as shown in Figure 3-1, vehicles located in the same segment form one cluster. The communication range will determine the size of a one-hop cluster. If a vehicle is in an ECA, it joins the cluster for this ECA and performs V2V communications. That means packets are first forwarded to the closest CN and this CN relays packets to the adjacent cluster which is closer to the destination. A semi-truck usually deploys several sensors in its trailer, and these sensors will form an intra-vehicle communication network. For this sensor network, a static cluster is formed and CN will be the central controller in the tractor of the semi-trailer that provides information to the driver.

The network partition information can be integrated into current digital maps used for GPS navigation systems. It can be pre-installed in the digital maps or downloaded in real-time from a roadside infrastructure. Because GPS navigation systems will likely become a standard component in future vehicles, it is assumed that the vehicle is able to obtain its real-time location and decides if it is necessary to join/create a cluster.

A CN is elected for each segment in a distributed way. Within a certain ECA, every node computes an Initial Electing Factor (IEF) that reflects the expected time to be spent in this ECA. Then, it waits for a backoff duration which is inversely proportional to its IEF before broadcasting a CN selection message. If a node receives a CN selection message from others before it times out, it sets its own states to a member and registers the information of the new CN. A cluster can be formed in two different ways: proactive and passive. In the proactive mode, clusters are always created for all ECAs even if there is no data communication within this ECA. The drawback of this method is that too much network overhead is involved. To address this issue, clusters can be reactively built only when there is request for data communications. For the sensor networks in a semi-truck, a distributed address assignment mechanism will be used to form a hierarchical network topology and the sink (center controller) will serve as the CN.

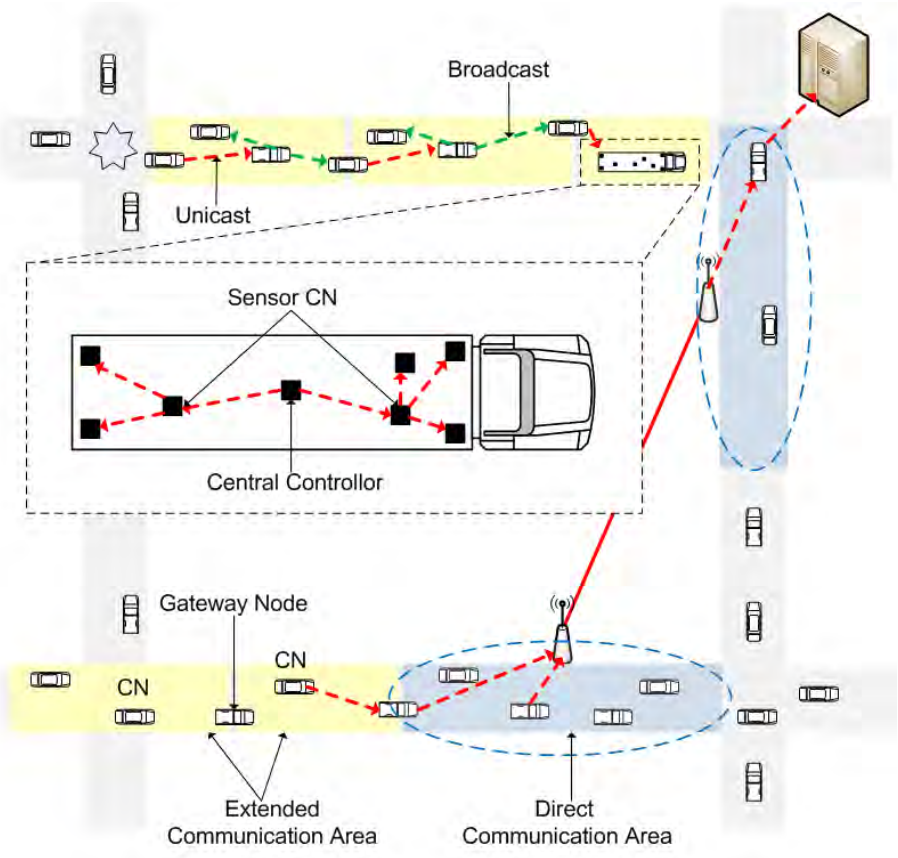

Figure 3-1. Diagram. Integrated Vehicle Network Architecture.

3.2 Channel Management for Vehicle Wireless Networks

3.2.1 Channel Management for Integrated Vehicle Network

Under normal conditions, communicating devices will exchange small control messages to reserve the channels and prevent other devices from interfering with their communication. In V2I, IN (roadside) will manage the channel reservation, whereas in V2V, CN will manage the channel reservation similar to INs, for ordinary nodes and gateway nodes (that interconnect clusters). In intra-vehicle network, the CN (usually at the tractor) will manage the channel reservation for sensor communication at the trailers. All INs and CNs in the vicinity will coordinate together to manage channel allocation to avoid interference. Hence the channel reservation algorithm is integrated for V2V, V2I and intra-vehicle network clusters to avoid interference among these communication types.

However, despite these schemes, external interference could still occur, in which case the system will accurately determine if interference (and not channel fading) is the actual cause of transmission degradation, in which case the automatic channel hopping algorithm will select a new channel that will avoid the interference channels (may be caused by external sources). When interference is the cause of degradation in delivery ratio, the transmission is maintained at the current rate, but when channel fading is determined to be the actual cause of transmission degradation, then the transmission rate is reduced in order to improve the delivery ratio, i.e. reduce packet error rate, thus improving the vehicular network robustness. However radio occlusion, for example, from the trailer of the semi-truck or severe fading problem persists, then the delivery rate will still be low, particularly for direct transmission between sensors at the rear of the trailer and controllers at the front of the truck. In this case, reliable multi-hop forwarding through intermediate nodes on the trailer and truck will ensure reliable transmission between these nodes. The routing algorithm selects the multi-hop path which provides the best transmission quality and network connectivity for forwarding packets. The network connectivity information will first be modeled based upon statistical network density data, and then be updated after real-time density information is collected.

3.2.2 Channel Management for ECAs

In dealing with wireless clusters, a channel reservation algorithm for assigning channels to the various clusters that are formed dynamically was developed. The assumption here is that the clusters have been formed and an election algorithm has been used to select a cluster head for each cluster.

Each cluster is assigned a communication channel. The assignment can be done in such a way so that only orthogonal channels are used. Assuming IEEE 802.11g is used, then there are only three orthogonal channels: 1, 6 and 11. The simplest way of assignment of channels can be as shown in Figure 3-2 where channels 1, 6 and 11 are assigned in sequence to the adjacent clusters, again followed by channels 1,6,11,1,6,11 and so on.

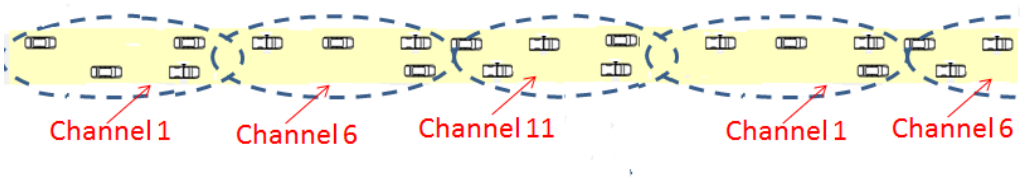

Figure 3-2. Diagram. Channel Assignment in Roads without Intersection.

However, in roads that involve intersections as shown in Figure 3-3, then all the nearby clusters need to be taken into consideration. Then there is a need to look into an elaborative channel assignment design techniques. Another issue is whether the two clusters should be using each other's data for selecting their channel or they need to do it on their own without any control data. There can be a central entity which can guide the cluster heads as to which is the most appropriate channel to be used.

The channel assignment can be either coordinated or un-coordinated. In an uncoordinated environment, two or more adjacent clusters can have either the same channels or adjacent channels. The same channels on nearby clusters can cause co-channel interference while the adjacent channel on nearby clusters may reduce the network performance due to adjacent channel interference. The adjacent channel interference problem can be eliminated by using only orthogonal channels in the channel assignment scheme. Since reducing the co-channel interference requires a coordination algorithm, this type of algorithm in difficult to implement in the un-coordinated environment.

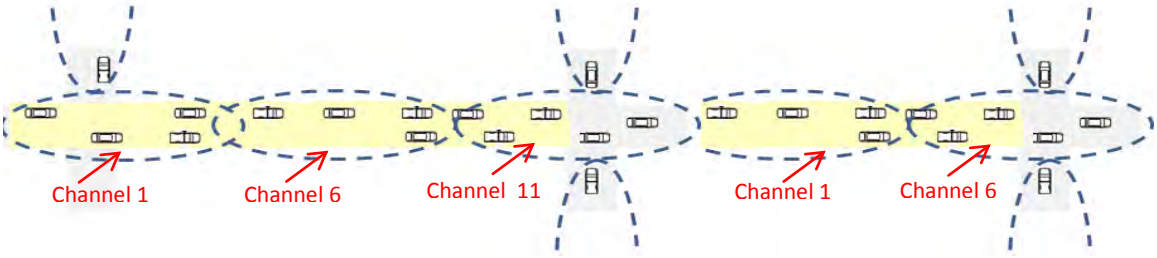

Figure 3-3. Diagram. Channel Assignment with Road Intersection.

In un-coordinated systems, the cluster head will just independently select the communication channel in which it senses the least number of clients (Achanta, 2006). In this case, the cluster head will have to sniff the traffic on all the orthogonal channels. (Taking all channels will add the adjacent channel interference which is being avoided here.) Then the cluster head will periodically select the channel with the least traffic.

The main performance metric that is considered here is the co-channel interference. So to reduce the co-channel interference, a scheme based on the vertex coloring algorithm can be used

(Mahonen et al., 2004). The vertex coloring algorithm can be used when assigning a channel to a cluster which is surrounded by two other clusters. Consider the two clusters use Channel 1 and Channel 6, then the cluster under consideration can be assigned Channel 11. Until and unless the traffic movement is high in the given region, this greedy strategy can help solve the co-channel interference up to a point.

Furthermore, for the coordinated environment, a communication channel is required to exchange control information. This channel needs to be separate from the other communicating channels used for data transmission. Following the example of cellular networks, which has two separate channels for data (voice) and control information, the idea can be replicated using a particular channel for only transmitting control information between the cluster heads of the cluster. For a 2.4 GHz band where there are only three orthogonal channels, this does not seem a good idea but for 5 GHz band, such as in IEEE 802.11a where there are 12 orthogonal channels, one channel can always be dedicated for control information.

Some other metrics such as load balancing as in the cellular networks can be considered too. However, satisfying this requirement might add to the overhead as a cost for raising performance. In such cases, the implementation model can be implemented by considering the interference factor at the other nodes (Mishra et al., 2006) of the cluster instead of the cluster head. Though it can give a better performance, it incurs quite an overhead for the ever-changing mobile network environments.

3.3 Platforms for Vehicle Wireless Networks

The configurations of the wireless hardware for implementing wireless vehicle networks consists of a Mini-ITX (Model NM10-A-E), manufactured by ZOTAC, with Intel Atom D510 1.66 GHz Dual-core CPU and 4 GB memory. In these experiments, two IEEE 802.11n wireless cards were tested: Ubiquiti SR71-E (Atheros AR9280 chipset) and Intel Centrino N6200. Both of them support most functions provided by the IEEE 802.11n standard. The storage on the platform is a solid state disk 50 GB hard drive.

Since cost efficiency is important in intra-vehicle communications, standard commercial omnidirectional antennas were used in the experiment: D-Link 7 dBi omni-directional antenna (ANT24-0700). Most commercial IEEE 802.11n radios are designed for indoor use and are limited to 100 mW, which is smaller than the outdoor radios (1W). On the other hand, transmitting at high power outputs will result in very low data rates due to delay spread, which is the time delay in which reflected radio signals arrive after the direct signal has arrived at the receiver. Since delay spread will cause interference with other symbols in the same transmission stream, a lower data rate is required to avoid interference. Hence, very few high-power IEEE 802.11n radios are available for outdoor environments. Most wireless IEEE 802.11n radios transmit using low-gain vertical omni-directional dipole antennas such as the D-Link 7 dBi used in this project.

This page intentionally left blank.

Chapter 4 – Secure Wireless Vehicle Networks

4.1 Security Problems in Wireless Vehicle Networks

In a typical wireless link between the AP and a station, WLAN does not provide sufficient end-to-end security for critical data packet transmissions. Initially, Wired Equivalent Privacy (WEP) was designed by IEEE to provide the basic security services of authentication, confidentiality and integrity. WEP does not address many security issues such as audit, authorization, replay protection, non-repudiation and key management. The lack of key management services is particularly problematic. To overcome these drawbacks, IEEE 802.11i standard has been defined. IEEE 802.11i is a well-designed standard providing mutual authentication, confidentiality and integrity. It assures security not only for the data frames but also the control and management frames (Ferreri et al., 2004).

Consider the following security problem in typical vehicle networks which has no security protocol. Assume that a malicious attacker enters the wireless vehicle network (Figure 4-1). The attacker can spoof the address of any of the stations connected to the AP, then change its MAC address to impersonate a legitimate station and can get connected to the AP. Note: In this case there are two stations with the same MAC address connected to the AP. So when the AP sends out information for that particular station, both the legitimate as well as the illegitimate station can receive this information. Also, the illegitimate station can send a dissociation request and can get itself as well as the legitimate station disassociated (disconnected) from the AP.

Another form of malicious attacker may jam the wireless channels being used by the vehicles for communication. There are many different types of jamming attacks which can be categorized as proactive jammers and reactive jammers. Proactive jammers will constantly jam the channel regardless of whether the vehicles are transmitting in that channel or not. Reactive jammers, however, jam the channel only when it detects normal transmission by vehicles using the wireless network. Both proactive and reactive jamming attacks result in what is called DoS attacks since they disrupt wireless communication and prevents critical messages from being received by the intended vehicle or sensor data from being received by the electronic control system.

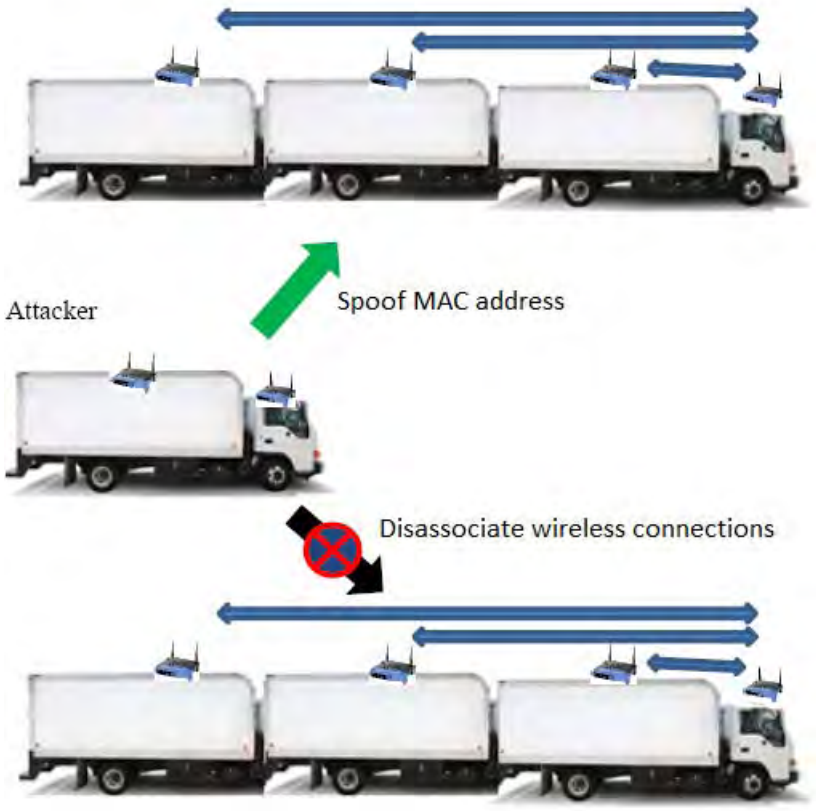

Figure 4-1. Diagram. Security Problem in Vehicle Wireless Networks.

4.2 Techniques for Overcoming Security Problems

Secure communication link based on IEEE 802.11i and other jamming counter measures are used to overcome security problems. The IEEE 802.11i introduced the concept of a Robust Security Network (RSN). It has three components: 802.1X for authentication making use of Extensible Authentication Protocol (EAP), RSN for keeping track of associations, and Advanced Encryption Standard (AES) based CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). 802.11i authentication uses 802.1X scheme, while the traffic is encrypted using Temporal Key Integrity Protocol (TKIP), or CCMP. 802.11i provides mutual authentication between the supplicant and the authenticator (He and Mitchell, 2004). Completion of the authentication process means that the supplicant and the authenticator verify each other's identity and generate session keys which are further used for secure data communication (Xing et al., 2008). An RSN is defined as a wireless security network that only allows the creation of Robust Security Network Associations (RSNA) (He and Mitchell, 2005).

First, the IEEE 802.11i standard framework and processes will be described and then possible attacks in 802.11i will be identified. Lastly, existing solutions will be discussed as well as

analyses provided. The following describes the IEEE 802.11i authentication and key management protocols.

The RSNA procedure consists of IEEE 802.1X key management protocols and authentication. Its authentication process involves three entities: supplicant or station (STA), AP or authenticator and authentication server. As shown in Figure 4-2, there are six steps involved in the procedure: (1) Network Discovery, (2) Authentication and association, (3) EAP/802.1X/RADIUS Authentication, (4) 4-way handshake, (5) Group key handshake, and (6) Secure Data Communication (He et al., 2005).

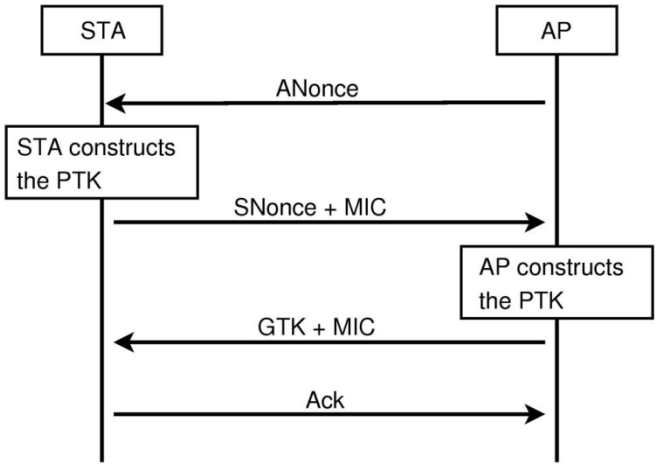

Figure 4-2. Diagram. IEEE 802.1X Authentication Process.

The following paragraphs describe these procedures in greater detail as mentioned in Yang et al. (2009) and He et al. (2005):

Phase 1: In the network discovery phase, either the AP broadcasts its security capabilities through the beacon frame; or the supplicant sends a probe request message to the AP, in response to which it will send its suite of authentication, cipher and key management.

Phase 2: In the authentication and association phase, the supplicant selects one AP from the list of available APs and attempts to authenticate and associate with it. The supplicant selects the suite as a part of the capabilities negotiation process to which the AP responds with success.

Phase 3: IEEE 802.1X is the chosen delivery mechanism for the IEEE 802.11i authentication. The actual authentication mechanism is provided by the encapsulation protocol EAP. The authentication method type of EAP is Transport Layer Security (TLS). EAPOL is a standard for passing EAP over a wired or wireless LAN. After this stage, the supplicant and authenticator have authenticated each other and generate a shared secret, Master Session Key (MSK). The supplicant uses the MSK to generate the Pairwise Master Key (PMK), while the authentication server generates the same PMK and passes it to the authenticator.

Phase 4: In the 4-way handshake, PMK is taken as an input to this phase. PMK can be derived from stage 3 or a cached PMK can be used or a Pre-Shared Key (PSK). Fresh Pairwise Transient Keys (PTK) are generated using a random function generator, which takes input: PMK, MAC addresses and nonces of supplicant and authenticator both. PTK generated here is divided into Key Encryption Key (KEK), Key Confirmation Key (KCK) and temporal key. These keys are used in the secure (encrypted) data communication through the TKIP and CCMP protocols.

Phase 5: Group-Key handshake; which is an optional stage. In case of multicast applications, the authenticator generates a Group Transient Key (GTK). A fresh GTK is generated and distributed to the supplicants.

Phase 6: Secure Data communication; in which the PTK or GTK is used for the exchange of protected data packets using data confidentiality protocols.

The main difference that distinguished Wi-Fi Protected Access (WPA) from WEP is as follows. These WPA networks use EAP to authenticate a user before it is allowed access to the network (Yang et al., 2009). The smart design used by this 4-way handshake (Phase 4) is that a replay counter is added to each data frame. This replay counter will increase after each successful session. Though it provides no further optimizations, it plays an important role in preventing replay attacks in group key handshake (Wang and Srinivasan, 2010).

To counter jamming attacks that deny user wireless communication services, a method that can effectively avoid jamming attacks was investigated, using the dynamic channel hopping technique. Both proactive as well as reactive channel hopping techniques were investigated and their comparative performance was shown.

4.3 Implementation and Experimentation of WPA and IEEE 802.11i

The WPA and IEEE 802.11i protocol on the wireless devices used for vehicle communication were implemented. Using the implementation, experiments were conducted to collect performance data and evaluate the performance of IEEE 802.11i.

4.3.1 Overview of Different Types of WPA Authentication Techniques

Two types of WPA authentication were considered: WPA-EAP and WPA-PSK. WPA-EAP is a good choice for large businesses because it combines AP authentication with another layer of authentication through external authentication services. In contrast, WPA-PSK, which includes TKIP, is a good solution for small businesses, home networks, or small mobile networks, such as vehicle networks. WPA-PSK implements a mechanism involving a number of security keys, which is done through TKIP. If the intruder obtains one security key, he will not be able to use it for long because the TKIP system changes the security key used for data transmission every specified amount of time to prevent attempts at cracking the keys. The default Key Lifetime is usually set to either 30 or 60 min, which can also be changed.

The WPA-PSK version of the 802.11i authentication was implemented since it is more suitable for mobile wireless networks, such as vehicle networks. Also the performance of the secure wireless vehicle networks was measured and their performance was analyzed.

The experimental set up is as follows. The security type used is WPA 2 and the encryption type used is AES. WPA pairing is done using TKIP, whereas RSN pairing is done using CCMP 4-way handshake is the most important phase in IEEE 802.11i (IEEE 802.11i 2004).

4.3.2 Implementation of the WPA-PSK Authentication Process

The AP controls the authentication power in case of WPA-PSK. First, initial authentication is done using the PSK set in the wireless configuration. The key is set at the AP and then distributed by the administrator to clients. However, the PSK is only a basis for starting the detailed key-cipher generation process. Once the initial authentication is completed, then another so-called Master Key is generated which is bound to the particular session between the AP and the client.

The Master Key is then further split into so-called GTK which secures multicast and broadcast messages sent by the AP to the clients, and to another security key called PTK which secures the unicast messages sent from wireless clients to the AP. This algorithm has a very secure encryption mechanism called Advanced Encryption Standard - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). AES-CCMP is the most robust security encryption algorithm available.

IEEE 802.11i is the complete security protocol that is most commonly used to achieve the security goals: Confidentiality Integrity Availability (CIA). The PSKs are used for the integrity check of the clients connecting to the AP. The communication is made available after the AP has marked the client device as authenticated and associates with it, though availability is not one of the major goals of the IEEE 802.11i standard. WPA authentication includes the generation of the keys that are used to maintain the data confidentiality of the system by the AES-CCMP encryption mechanism.

The implementation of the WPA-PSK was installed on the AP using the *hostapd* daemon that is used for establishing an AP. For the WPA pairing, TKIP is used while CCMP is used for the RSN pairing. The major weakness of the IEEE 802.11i is the unencrypted management frames, which can be easily spoofed. To overcome that, another standard, IEEE 802.11w is defined. This standard has put forward some other weaknesses in the system which was not being looked into at this stage. The encryption of the management frames as made available by the standard 802.11w will only be considered. A patch was installed and the management frames being transmitted between the AP and the wireless client were encrypted, from 802.11w standard, on top of our IEEE 802.11i WPA security policies.

4.4 Results and Analysis of WPA and IEEE 802.11i Performance Evaluation

4.4.1 Execution Times of WPA Authentication Processes

First, the performance of IEEE 802.11i in two different cases is measured: (1) when the first station is connecting to the AP, and (2) when all other subsequent stations are connecting to the AP. In particular, the average elapse time for each phase of the protocol to execute is measured. Based on these execution time measurements, the two cases show some significant differences in the performance of the protocols.

Case 1: For the first station to get connected to the AP
The measurement results show that the time for association in Phase 2 takes approximately 65 ms on an average. The variation in the association time is between 40 to 80 ms. After association is complete, the session starts in one second. The measurement results show that the generation of the pairwise key takes on an average 400 μs.

Case 2: For all the other subsequent stations to get connected to the AP
In this case after the first station is connected to the AP, all other stations' association time take 30 ms. After the association is complete, sessions take 100-150 ms to start. Following that, the pairwise key is generated in about 100-120 μs. These results show that the elapse time for executing each phase of the protocol for all subsequent stations to connect to the AP is shorter than the time for the first station.

After the time the first station was connected to the AP, a group key handshake takes place between all the station and AP every 10 min. This time for periodic handshake is always the same, irrespective of the time when the second, third or other stations were connected to the AP.

In the case of insecure networks, for instance, without any security protocol, the re-association takes place between the AP and the station after every 45 s approximately.

4.4.2 Protection against Attack on Un-authenticated and Un-encrypted Management Frames

In analyzing the IEEE 802.11i and WPA protocols, it is determined that one of the security problems with these protocols is that the management frames are un-authenticated and un-encrypted. This renders even the IEEE 802.11i and WPA to be vulnerable at these points in the protocol. An attacker which spoofs the address of a legitimate station can impersonate its MAC address and send de-authentication or disassociation messages to the AP.

To protect the legitimate devices from getting disassociated or de-authenticated due to this, an additional functionality was added according to the hypothesis given in Wang and Srinivasan (2010.), which defers the de-authentication or disassociation by 5 s if the de-authentication or disassociation request is received before the pairwise key is generated.

As discussed above, the encryption of the management frames using the standard IEEE 802.11w was also considered. A patch was installed and the management frames being transmitted between the AP and the wireless client were encrypted, from IEEE 802.11w standard, on top of the IEEE 802.11i WPA security policies.

4.4.3 Performance Comparison between Authenticated System and Un-Authenticated Systems

Although the main advantage of the authentication algorithm is providing security, performance studies were done to compare the performance of systems that implement WPA authentication and systems that do not implement WPA authentication. The results of these studies show a trend towards improved performance in terms of throughput, data loss and transmission retries for systems that implement authentication. The system used in these studies is an IEEE 802.11g network which has the maximum specified throughput of 54 Mbps although the actual throughput that can be achieved in these systems is 27 Mbps.

Consider two trucks “A” and “B” (Figure 4-3), each of which has an intra-vehicle network where a client communicates with its AP through its wireless channel.

Figure 4-3. Diagram. Two Independent Intra-Vehicle Wireless Networks.

The graphs in Figure 4-4 and Figure 4-5 below show the maximum throughput that can be obtained by Truck A and Truck B when their wireless communication occur in isolation from each other, that is, the wireless signal from each truck does not interfere with the wireless transmission in the other.

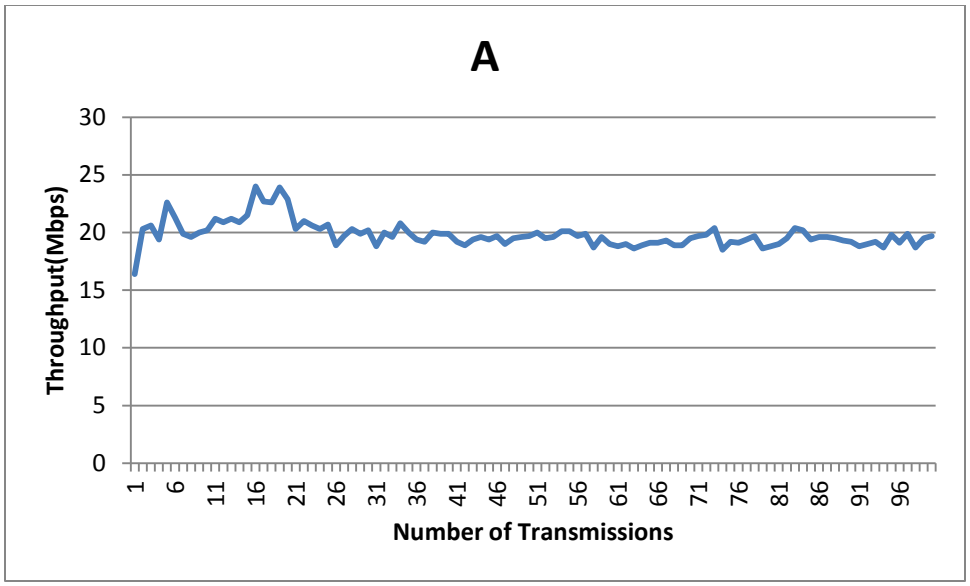

Figure 4-4. Graph. Throughput Performance of Truck A Intra-Vehicle Wireless Networks in Isolation.

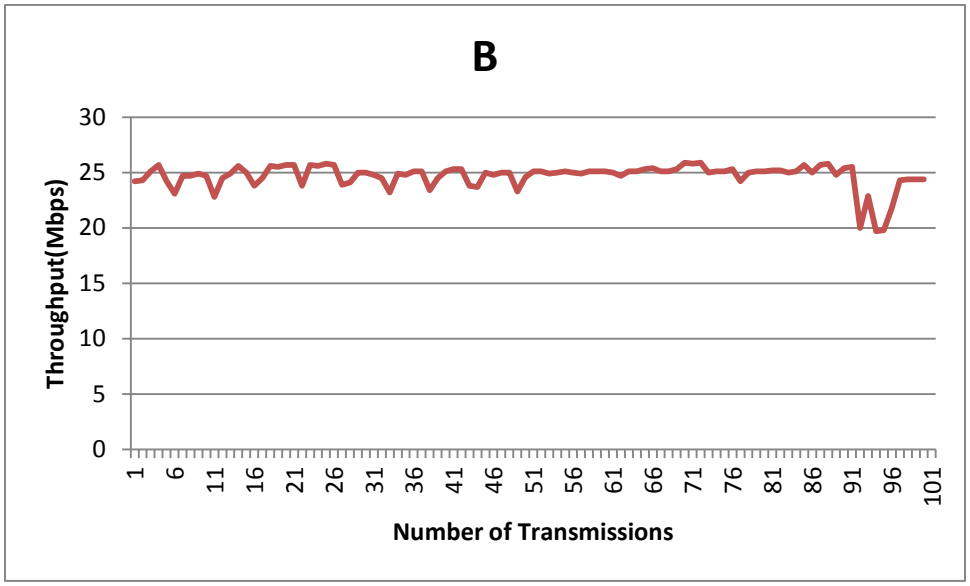

Figure 4-5. Graph. Throughput Performance of Truck B Intra-Vehicle Wireless Networks in Isolation.

In a second experiment, the networks in the two trucks were made to operate in each other's vicinity, where both trucks use the same communication channel. Both the trucks use un-authenticated networks for communication. The results in Figure 4-6 shows the throughput in the case where both the trucks use two separate non-authentication networks for transmitting data packets concurrently. The isolated performance of A was 20 Mbps on an average and that of B was 25 Mbps, but when they operate together and in close proximity, they end up with 8 Mbps

and 16 Mbps respectively. The weaker network is pushed down while the stronger one maintains a high average rate.

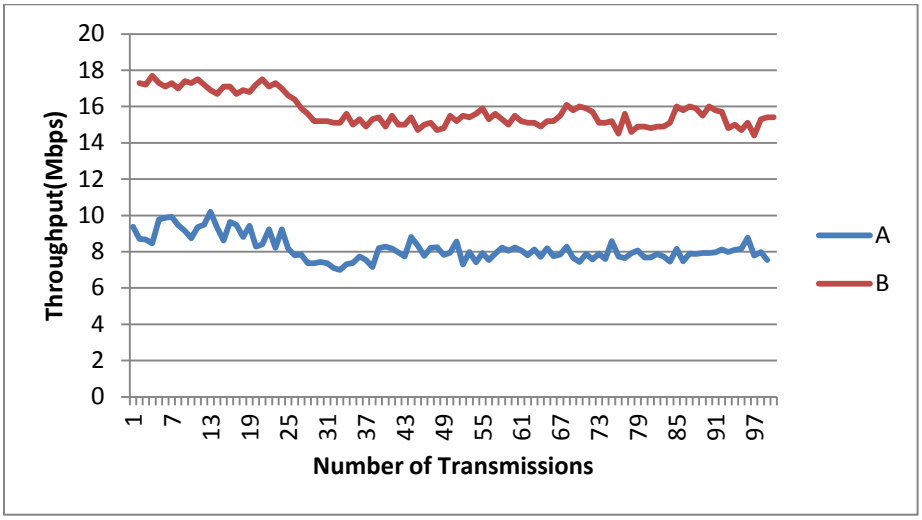

Figure 4-6. Graph. Throughput of Truck A and B Un-Authenticated Wireless Networks in Close Proximity.

In the third experiment, WPA-PSK authentication was used for both Truck A and B wireless networks as is described above. The graphs in Figure 4-7 shows the performance that was obtained with authenticated networks. Truck B still has better performance than Truck A, but Truck A throughput has risen from 8 Mbps average to 10 Mbps whereas Truck B throughput has dropped from 16 Mbps to 14.5 Mbps. This shows that with authentication, both the networks have been given an equal share of bandwidth to use.

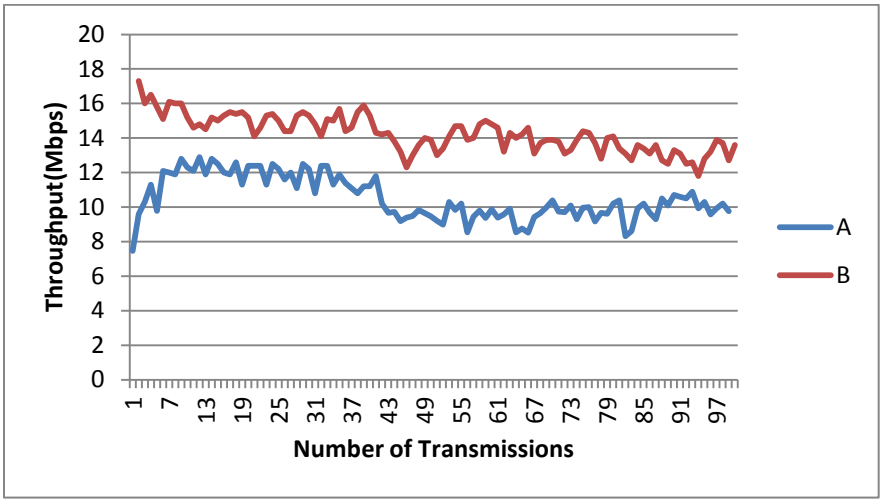

Figure 4-7. Graph. Throughput of Truck A and B Authenticated Wireless Networks in Close Proximity.

These tests were completed numerous times and sometimes a few packets were dropped when the network is not authenticated whereas in authenticated networks this was not the case. This shows that authenticated wireless networks has higher reliability.

Moreover, the above authentication setup used a non-orthogonal (but same) channel for both the networks. In the fourth experiment, the change in the performance was further investigated when any of the orthogonal channels were used, such as Channel 1, 6 or 11 in the following way. Here, as shown in Figure 4-8, the differences between the throughputs of both the networks have been reduced.

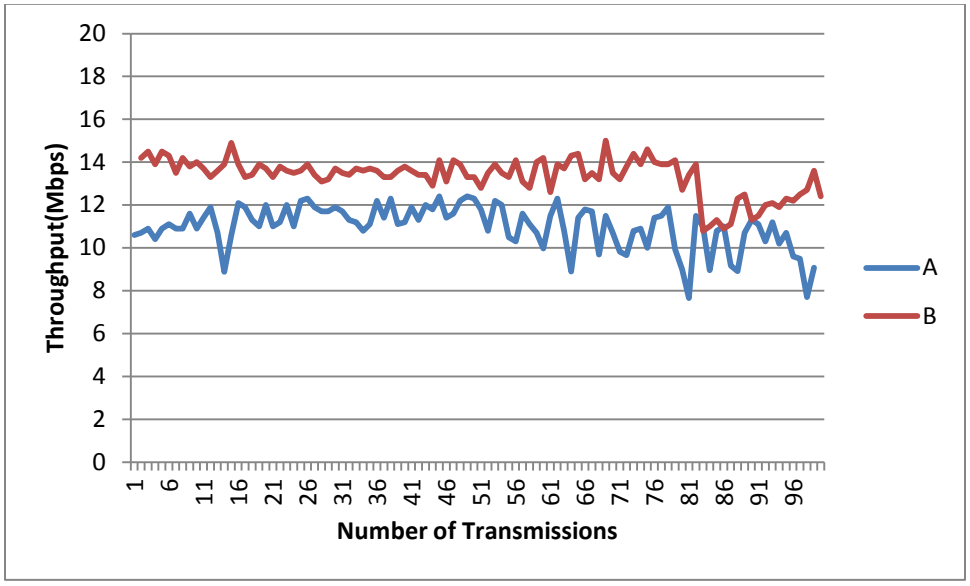

Figure 4-8. Graph. Throughput of Truck A and B Authenticated Wireless Networks with Same Orthogonal Channels.

In all the above experiments, the two trucks have been operating on the same channel, whether it is non-orthogonal or orthogonal. In this fifth experiment, the two trucks were set to work on two different orthogonal channels. The results in Figure 4-9 show that there is again a further reduction in the differences of the throughput performance of the two trucks' wireless networks.

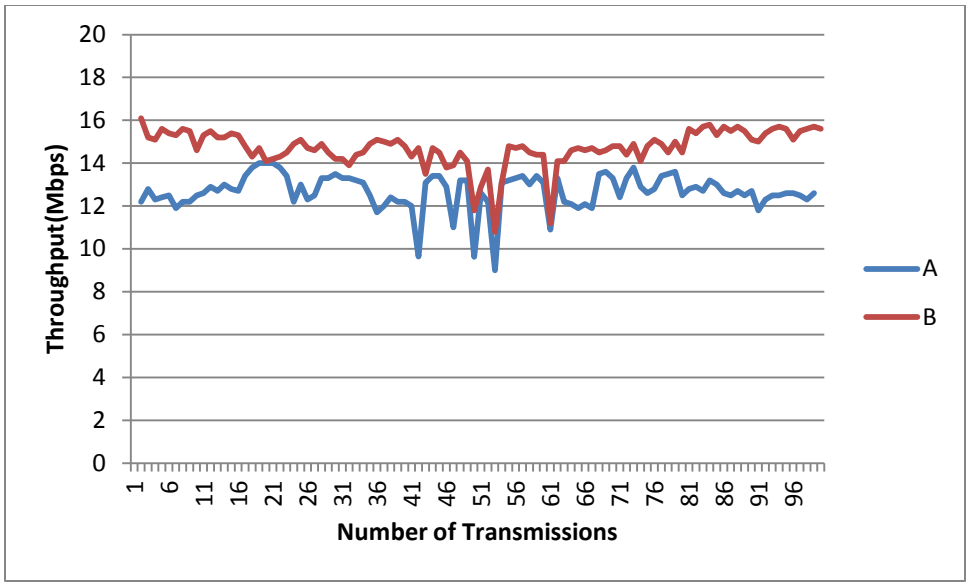

Figure 4-9. Graph. Throughput of Truck A and B Authenticated Networks with Two Different Orthogonal Channels.

In the sixth experiment, the data loss of the non-authenticated was compared to that of the authenticated systems. As shown in Figure 4-10, there is no major data loss seen in either but in authenticated systems the data loss is practically zero while in non-authenticated systems there is a slight data loss as indicated in the graph.

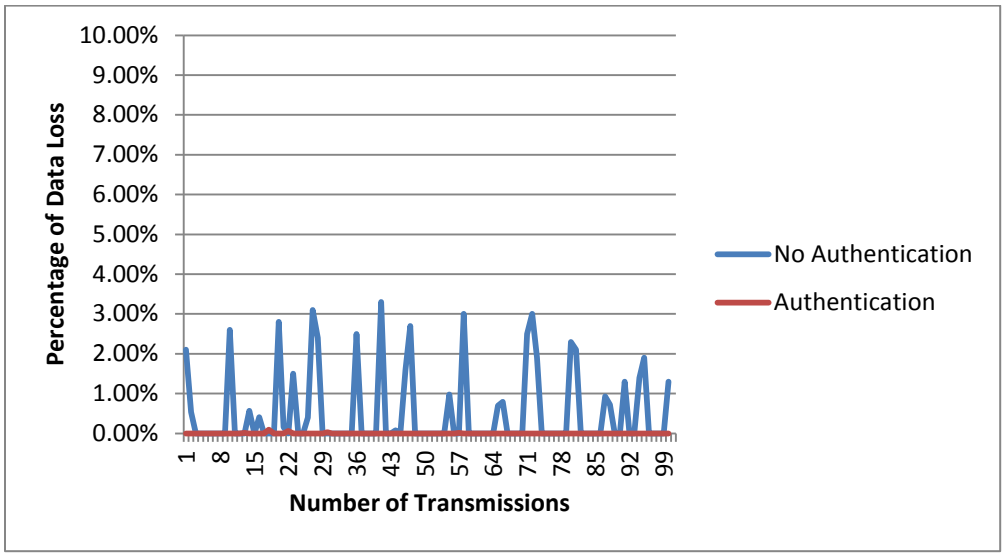

Figure 4-10. Graph. Data loss of Authenticated and Un-Authenticated Wireless Networks.

4.5 Implementation of Dynamic Channel Hopping

To avoid jamming attacks on the wireless vehicle network, the dynamic channel hopping was implemented as a software module. There are two forms of dynamic channel hopping: proactive

and reactive. Channel hopping can be proactive in that switching occurs at fixed time periods that are independent of channel performance. On the other hand, channel hopping can also be reactive in that switching occurs when the performance of a channel becomes particularly poor or when a specific attack has been detected.

4.6 Results and Analysis of Dynamic Channel Hopping

Experiments were conducted to determine the throughput performance of proactive in comparison with reactive channel hopping. This allowed for the estimation of the throughput that can be supported by each different channel hopping countermeasure to jamming.

4.6.1 Results of Proactive Channel Hopping Performance

When the proactive channel hopping protocol is set to switch channel every 10 s, the results show that the average throughput is about 16 Mbps. However, there are frequent drops in the throughput to 14 Mbps. The result of the graph of the throughput is shown in Figure 4-11, which also indicates the regular period in which the channel is switched. The breaks in the throughput graphs indicate the time in which a channel is switched to another channel at every 10 s interval. Subsequent graphs also indicate these switching times, although at different time interval.

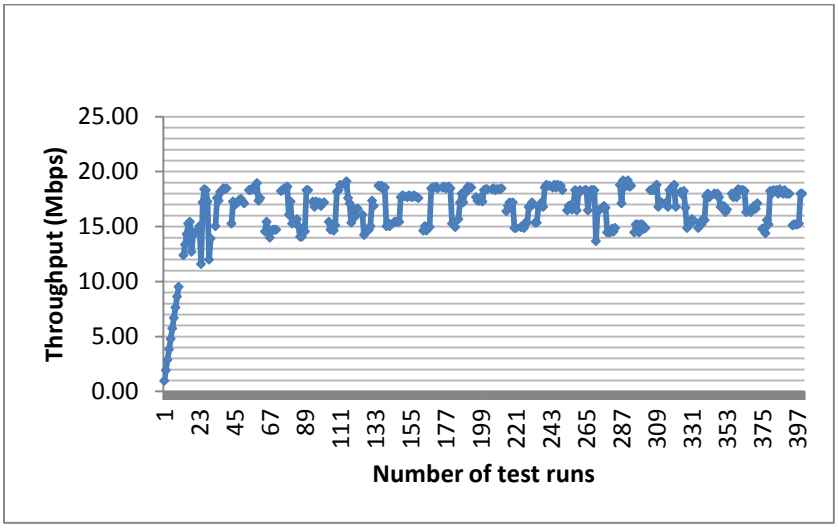

Figure 4-11. Graph. Proactive Channel Hopping with 10 Seconds Switching Interval.

When the proactive channel hopping protocol is set to switch channel every 20 s, the results in Figure 4-12 show that the average throughput is still at about 16 Mbps, which is similar to the throughput when the switching time is 10 s. However, there are fewer drops to low throughput of about 15 Mbps.

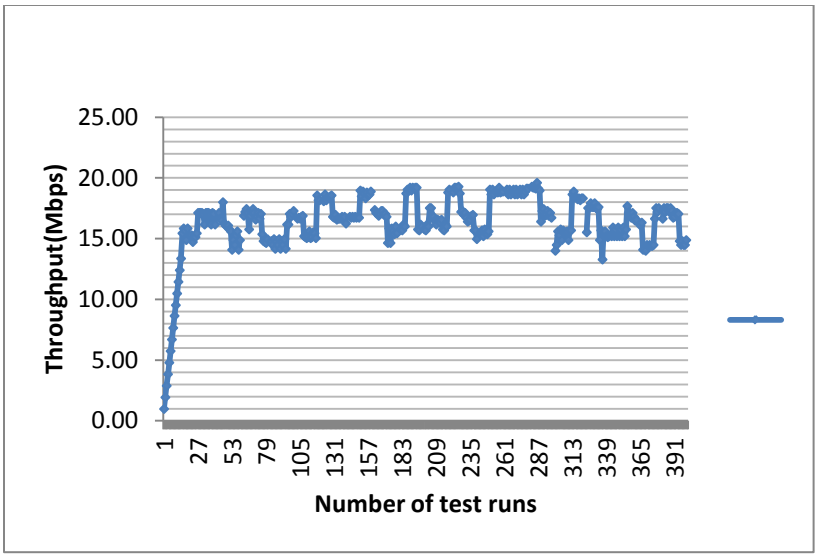

Figure 4-12. Graph. Proactive Channel Hopping with 20 Seconds Switching Interval.

When the proactive channel hopping protocol is set to switch channel every 30 s, the results in Figure 4-13 show that the average throughput is about 17 Mbps, which is slightly better than the throughput when the switching time is 20 s. However, there are fewer drops to low throughput and the throughput remains more consistent between 16 and 18 Mbps.

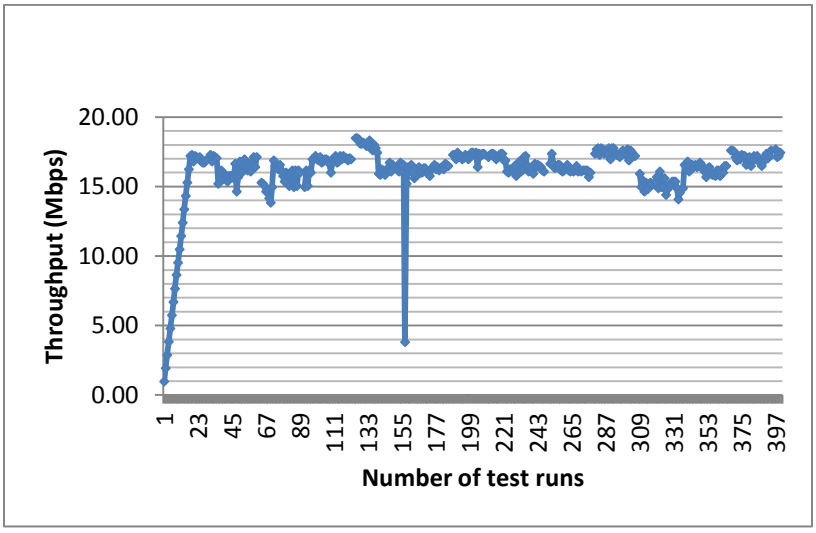

Figure 4-13. Graph. Proactive Channel Hopping with 30 Seconds Switching Interval.

Discussion on Proactive Channel Hopping Performance

From the above results it can be interpreted that the longer the time interval for switching channels, the better is the throughput performance. With time intervals of 10 s and 20 s a lot of

random drops in throughput are seen, whereas with time interval of 30 s for switching channels, the throughput is more consistently higher.

4.6.2 Results of Reactive Channel Hopping Performance

For the reactive channel hopping, the channel utilization parameter was used to measure the interference and jamming on the channel (ACS, 2011). Very high channel utilization is an indication that the channel could be jammed or has extremely high interfering signals. When the channel utilization is above a certain threshold for the current channel in use, the reactive channel hopping algorithm will find another optimal channel that utilization that is lower than the threshold. Channel utilization is calculated in Figure 4-14.

Channel Utilization = (channel busy time – channel transmission time) / (channel active time – channel transmission time)

Figure 4-14. Equation. Calculation for Channel Utilization.

Figure 4-15 shows the results of the throughput generated by the reactive channel hopping algorithm with channel utilization check. The throughput performance fluctuates between 15 and 21 Mbps.

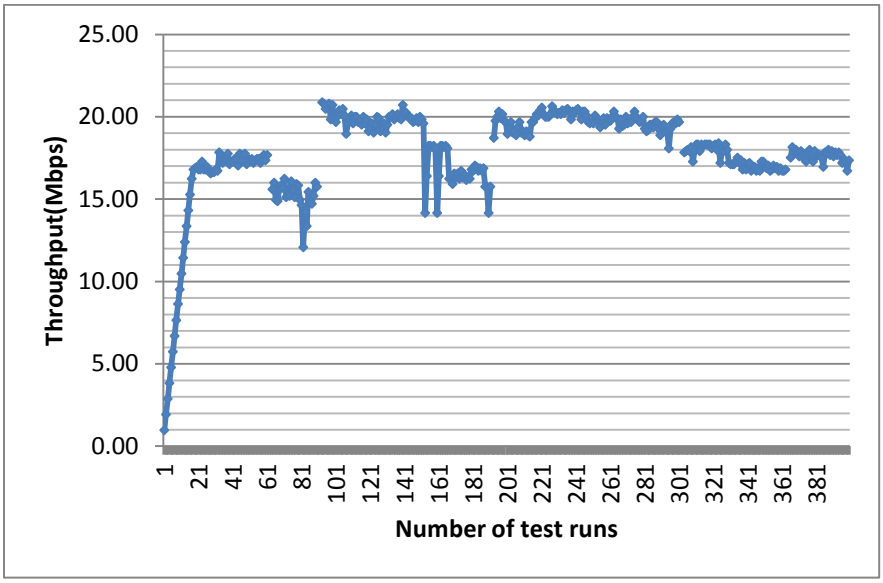

Figure 4-15. Graph. Reactive Channel Hopping with Channel Utilization Check.

Reactive Channel Hopping with Channel Utilization and Retries Checks

In the next test, in addition to the channel utilization, the re-tries were also considered for deciding on when to switch channel. The higher the retries count, the poorer the quality of the channel which could mean the presence of a jamming signal or an interfering signal. A normal

test done every 10 s gives an average retry count of 125, while an every 1 s test gives an average retry count of 7. A 1 s test sends 87 to 89 data packets per second. Therefore, taking this into consideration, the threshold value for retries was set to 10 and 12.

The results in Figure 4-16 have similar throughput values as the above test in Figure 4-15 except that the number of switches taking place was more. The throughput performance still fluctuates between 15 and 21 Mbps but channel switching occurs twice as often as before.

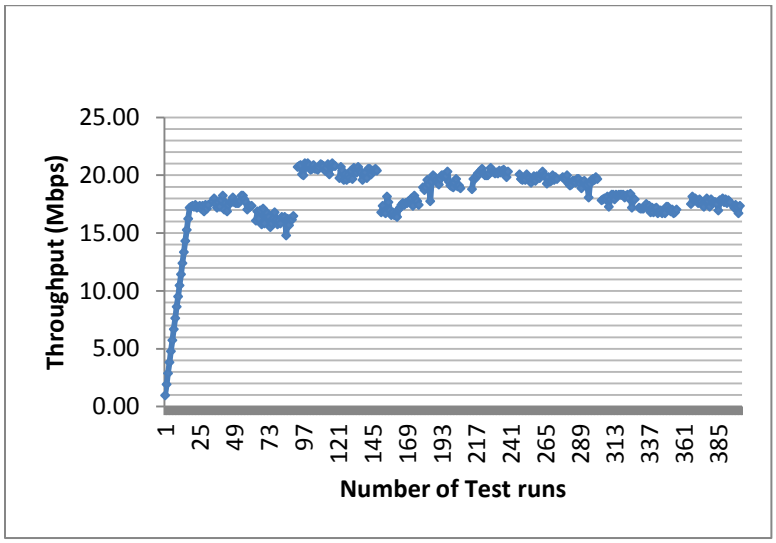

Figure 4-16. Graph. Reactive Channel Hopping with Channel Utilization Check and Retries.

Discussion of Comparison between Proactive and Reactive Channel Hopping Performance

The main results of comparing the performance between proactive and reactive channel hopping is that the maximum throughput values achieved with reactive hopping could reach up to 20 Mbps while with proactive channel hopping only 18 Mbps values were obtained. This result showed that reactive channel protocol can respond better and more quickly to jamming and interfering signals than proactive channel hopping. Note that in the experiments above, each test run is executed for 1 second.

Another experiment was conducted to compare the performance when using only orthogonal channels versus the performance when using all channels (some of which could be overlapping channels). The results of this test showed that there was no significant difference between the performance when orthogonal channels were made available for hopping and when using all the channels. The performance graphs, display the occurrence of channel hopping with a gap in the graph lines. After each channel hopping occurrence, the re-connection takes about 1 or 2 s.

This page intentionally left blank.

Chapter 5 – Reliable Wireless Vehicle Networks

5.1 Reliability Problems in Wireless Vehicle Networks

One of the major causes of reliability degradation in wireless networks is channel fading caused by long transmission distance or transmission being occluded by radio-opaque objects. Another major cause of unreliability in wireless networks is congestion due to excessive broadcast of data packets or simultaneous emergencies and alert messages as a result of critical events being sensed by many vehicles in the vicinity. Since transmission of critical emergencies messages must be reliably delivered to the vehicles involved over the wireless network, the networks must be developed to provide high level of reliability in guaranteeing packet delivery.

Besides channel fading and congestion above, other factors in the harsh operating environments of commercial vehicle wireless networks that may degrade transmission are mobility, APM, vibration, data packet collision, interference, and jamming. The technique for overcoming interference and jamming is dynamic channel hopping, discussed in Section 4.5. Other techniques are described below.

5.2 Requirements for Wireless Communication in Vehicle ESC

To implement wireless intra-vehicle networks, first it must be calculated what the minimum raw data rates are for the transmission of sensor and actuator control data in a wireless vehicle ESC network. Since the minimum data rate does not consider packet loss, higher data rates would be necessary to handle retransmissions due to packet loss. By estimating the packet loss and minimum data rate, the actual data rate that is required can be derived.

The wireless communication link between the trailer controller and the tractor controller supports transmission of sensor data from the trailer to the tractor and control data in the reverse direction. Each sensor data packet contains all the desired vehicle parameters, whereby the total minimum sensor data packet size is 30 B. Each sensor data packet contains the following sensor information:

- Trailer Ax, Ay, and Az (3 B)
- Trailer Angular Rate (yaw, roll, pitch) (3 B)
- Trailer Angle (yaw, roll, pitch) (5 B)
- Trailer Position (Latitude, Longitude) (16 B)
- Two Trailer Wheel Speeds (2 B)
- Air Suspension Load (2 B).

Since side slip can be calculated from the yaw rate, lateral acceleration, and GPS data, these sensor data include all the state and vehicle parameters that are required for ESC as described in Section 3.2.2. The total number of B of sensor data in each packet is 31 B. Assuming that the sensor and control data are transmitted through Transmission Control Protocol (TCP) for reliability, then the additional header sizes for TCP, Internet Protocol (IP), and IEEE 802.11n are 20 B, 20 B, and 34 B, respectively. Hence, the total number of bytes in each sensor data packet is 31+20+20+34 B (i.e. 105 B or 105x8 b). Since the update rate of the sensor data is 100 Hz, the minimum required bandwidth for the wireless sensor data transmission is 105x8x100 b/s (i.e. 84 kbps). This required bandwidth for ESC is well below the 24 Mbps transmission rate of IEEE 802.11g, even with a high packet drop rate. This rate is comparable to the typical baud rate of On-Board Dagnostics (OBD) systems, 100 kbps. From experience, there is a packet drop rate below 10% transmission over distances between 30 to 50 m. Assuming that a retransmission is sufficient to retransmit dropped packets, then the actual sensor rate is 84 x 1.1 kbps (i.e. 92.4 kbps). Although the drop rate could be higher in the harsh tractor-trailer environment, the required transmission should still be supported. The wireless transmission tests on the actual Longer Combination Vehicle (LCV) environment show packet loss rates of less than 10% and transmission throughput of about 40 Mbps. Other road and weather conditions may cause weak transmission and disconnections due to interference, collisions, non-line of sight problems (occlusion), and channel fading. Attenuation from heavy rain will likely cause a drop in the transmission throughput, although experiments were not conducted to measure throughput degradation due to rain. Future work should include more tests in poor weather conditions to determine how much the throughput will drop due to different inclement weather conditions and the effects of splash and spray on the wireless transmission.

The packet size of the control data is 2 B. Each control packet contains the following control data: Left Side Brakes (1 B) and Right Side Brakes (1 B). When added to the additional header for TCP (20 B), IP (20 B), and IEEE 802.11n (34 B), then the total packet size of the control data packet is 2+20+20+34 B (i.e. 76 B or 76x8 b). With the update rate of 100 Hz for control data, then the total minimum bandwidth required is 76x8x100 bps (i.e. 60.8 kbps. Again, if the packet drop rate is 10% and that only one retransmission is required for each dropped packet, then the actual control data rate is 66.9 kbps. Thus the total required bandwidth for both the sensor and control data is 158.4 kbps. This is again well below the 40 Mbps transmission rate of IEEE 802.11n.

The total delay for transmitting each sensor signal or data packet should include transmission time, propagation, and processing delay. From the field measurements, the total delay for each packet transmission is typically 1 or 2 ms. The transmission delay is very small (i.e., less than 0.03 ms) based on the packet size of 832 b for all the vehicle sensor parameters as listed above, and the transmission rate of 40 Mbps.

The above delay is based on a packet drop rate of less than 10% for the distance of 30 to 50 m as measured during this project. However, if the transmission channel is weak, higher drop rates

and retransmissions will result and will increase the latency to possibly 10 ms for each packet transmission.

5.3 Techniques for Improving Reliability of Wireless Vehicle Networks

In this section the techniques for reliable wireless networks based on multi-hop packet forwarding and efficient broadcast will be discussed.

5.3.1 Reliable Multi-Hop Packet Forwarding Protocol

One of the methods to overcome channel fading due to transmission distance or occlusion is to provide capabilities for alternate and shorter routes through multi-hop wireless packet forwarding. Since each link in multi-hop routing is shorter than single hop, the channel quality is higher and the transmission is more reliable.

This method for reliable multi-hop packet forwarding is used when the system determines that wireless transmission over a single link results in a severe fading problem, possibly due to distance or reduced transmission power. Severe fading problems may also occur when there is radio occlusion, such as from the trailer to the tractor, or occlusion between vehicles. When severe channel fading occurs, rate adaptation methods will not help. In this case, reliable multi-hop forwarding through intermediate nodes on the trailer and truck will ensure reliable transmission between these nodes (each node represents a device that is equipped with wireless transceiver, antenna, processor, and storage). The routing algorithm selects the multi-hop path that provides the best transmission quality and network connectivity for forwarding packets. The network connectivity information will first be modeled based upon statistical network density data, and then will be updated after real-time density information is collected. Because in the multi-hop scheme, the distance between nodes in each hop is relatively short, the transmission reliability is relatively high. Hence reliable transmission of sensor and actuator data can be achieved using multiple short but reliable wireless links.

5.3.2 Efficient Broadcast Protocol

Another method for improving reliability to overcome broadcast congestion is to provide efficient method for broadcasting emergency messages. Excessive message broadcast will cause some data packets to be dropped because of the high traffic throughput the intermediate nodes. Efficient broadcast instead reduces the number of packets in the network by aggregating broadcast packets at intermediate nodes and then re-broadcasting them to other nodes.

Broadcast packets such as emergency messages may cause congestion in wireless channels. In order to improve performance in these highly congested wireless conditions, a more efficient broadcast protocol is required to reduce congestion and improve throughput. To demonstrate the feasibility of more efficient broadcast protocol, the Auburn University vehicle wireless network team developed an efficient broadcast protocol that aggregates broadcast packets at intermediate nodes and then re-broadcasts them to others. The hierarchical aggregation of observations was

used from dissemination-based, distributed traffic information systems. Instead of carrying specific values, the aggregates contain a probabilistic approximation. This scheme can overcome two central problems of existing aggregation schemes for vehicular networks. First, when multiple aggregates of observations for the same area are available, it is possible to combine them into an aggregate containing all information from the original aggregates. Second, any observation or aggregate can be included into higher level aggregates, regardless of whether it has already been previously added. Using this efficient broadcast protocol, the number of packets in the wireless networks can be reduced, thus improving the throughput and reliability.

5.4 Implementation of Reliable Multi-hop Packet Forwarding

The multi-hop protocol is implemented at the application layer using User Datagram Protocol (UDP) socket programming libraries. Since it is implemented at the application layer, the communication time is slightly longer than if it were implemented at the network layer (Figure 5-1). However, network layer implementation is more complex and kernel debugging is more time consuming. This application layer implementation could be re-implemented at the network layer in the actual software distribution, where efficiency is important. (Standard computer networks are organized into hierarchical layers where each layer provides different networking functions. The application layer provides application-specific services, such as file transfer and web access services. The transport layer provides end-to-end communication services that can be either connection-oriented or connectionless. The network layer provides inter-networking services, such as routing and addressing. The media access control layer provides methods for coordination of transmission between communication devices through a medium. The PHY layer provides the methods for actual transmission of the signals representing the data that are being communicated.)

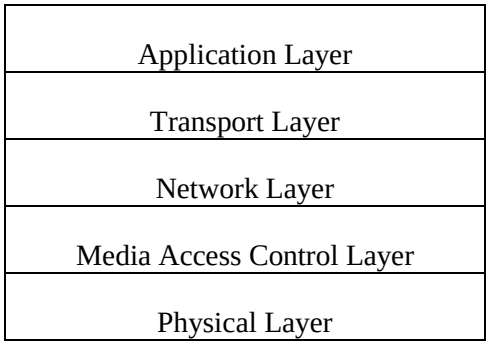

Figure 5-1. Diagram. Network Architecture.

The implementation of the multi-hop protocol execution was tested on four Mini-ITXs (Model NM10-A-E), manufactured by ZOTAC, with Intel Atom D510 1.66 GHz Dual-core CPU and 4 GB memory. In the multi-hop experiments, Ubiquiti SR71-E (Atheros AR9280 chipset) IEEE 802.11n wireless cards were experimented with. The wireless cards were configured in ad hoc

mode for the multi-hop protocol. For the purpose of the tests, the multi-hop protocol application uses static routing based on a configuration file.

For the purpose of measuring performance in terms of throughput, packet loss rate, and latency, the codes were implemented for collecting the necessary measurement data (e.g. number of packets and timestamps). To ensure that the timing of the four mini-ITXs is consistent, they were time synchronized with each other using Network Time Protocol daemon (NTPd). The timestamps were placed right before sending and right after receiving packets.

5.5 Implementation of Efficient Broadcast

To study the performance improvement of the implementation of the efficient broadcast protocol, many wireless nodes will be necessary. Since it is difficult to conduct these tests on the limited number of wireless nodes available, the test was conducted using a network simulation tool called ns-2. The ns-2 simulation tool is a discrete event simulator that is commonly used for simulation of routing protocols, particularly in ad-hoc networking research, and supports many popular network protocols. It offers simulation results for both wired and wireless networks. Using ns-2 simulation, the performance improvement can be studied of efficient broadcast over traditional broadcast when there are several hundred wireless nodes. When there are large numbers of broadcasting wireless stations, the performance can be reduced drastically. The efficient broadcast can alleviate this problem by reducing the number of packets being broadcast. The implementation of the efficient broadcast protocol on ns-2 can be easily re-implemented in the actual wireless devices when the need arises.

5.6 Experimentations and Simulations

Experiments were conducted to study the reliability and performance of wireless vehicle networks for under different wireless conditions and network configurations and measured their performance and reliability in terms of throughput and packet loss rate. Based on the analysis of these results, methods were developed for overcoming these wireless networking problems including a rate adaptation algorithm, multi-hop routing, and efficient broadcast with aggregation. The performance and reliability of these methods were measured and evaluated to show improvements.

5.6.1 Experimental Setups for Studying Performance of Wireless Vehicle Communication

Four main experimental setups were used for studying the performance of wireless vehicle communication using IEEE 802.11n:

1. The NCAT test track with a LCV (Figure 5-2)
2. Minivan on the I-85 highway
3. Static outdoor test environment beside Shelby Center at Auburn University
4. In a wireless networking laboratory

To compare performance and reliability, the experiments were conducted using wireless devices and network protocols based on a combination of different parameters as follows:

1. IEEE 802.11n wireless cards used were either Ubiquiti SR71-E or Intel Centrino N620
2. The frequencies tested were 2.4 GHz and 5.8 GHz
3. The rate adaptation algorithms studied were Fast Recovery Rate Adaptation (FRRA), “ath9k”, Minstrel, and fixed rate
4. Either one stream or two stream transmission was used
5. Three different antenna orientations were used.

The software used for measuring the performance of IEEE 802.11n transmission throughput and reliability is Iperf. The results of network throughput and data packet loss evaluations were collected for the different experimental setups to study the impact of each configuration and condition on IEEE 802.11n performance and reliability. The performance of a wireless intra-vehicle network can be affected by the surrounding conditions, interferences, and network congestion level. Variations of the performance results provided by Iperf provide a better understanding of the effect of different channel conditions and insights into how performance of IEEE 802.11n can be improved for intra-vehicle networks. To establish a baseline for all the measurements and eliminate effects of variation of channel conditions, the network throughput and packet loss was measured at 1.5m (5ft) range with an unobstructed line of sight before each experiment. When there was no variation in throughput and data loss results, different experiments commenced.

To study the effect of APM on wireless intra-vehicle networks, experiments were conducted with wireless transmission using a LCV running on the NCAT test track. Figure 5-2 shows the LCV and the NCAT test track used in the experiments. The wireless transmission tested was between the third trailer and the tractor, with a distance of about 30.5 m (100 ft). Figure 5-3 shows how the wireless controllers (Mini-ITXs) and the antennas are attached to the third trailer and were used in the experiment. In the figure, the wireless device shown is attached to the third trailer and a similar wireless device is attached to the tractor. The LCV moved at a speed of about 48.28 km/h (30 mph).

Each wireless controller is attached with two D-Link 7dBi antennas and connected to a Ublox LEA EVK-6T GPS. The triple tractor trailer was then driven around the NCAT track for about 15 min in each of two experiments. In the first experiment, the GPS data was recorded that were collected at the third trailer and transmitted wirelessly through IEEE 802.11n to the controller at the tractor. In the second experiment, as the triple tractor-trailer was driven around the NCAT track for 15 min, the wireless controllers ran Iperf tests with gradually increasing transmission rate (bandwidth). The results of these tests are discussed in Section 5.6.2 below.

Figure 5-2. Photograph. NCAT Test Track at Auburn University.

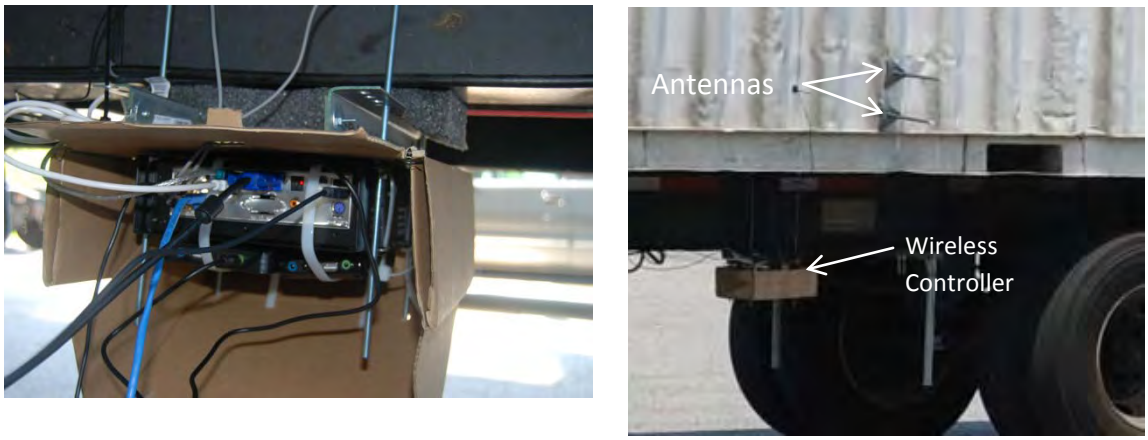

Figure 5-3. Photograph. Wireless Controller and Antennas Attached to the Third Trailer.

To study the effect of Spatial Multiplexing Malfunction (SMM) on network reliability, the experimental setup for wireless intra-vehicle road tests uses a mid-sized vehicle that is equipped with two IEEE 802.11n test platforms, with two antennas on each platform. One platform with two transmitting antennas is mounted on the rear right and another platform with two receiving ones on the front-right side of the vehicle. One static test and two road tests were conducted. The static test was conducted with the vehicle parked behind the Shelby Center Building at Auburn University. The road tests were conducted on the I-85 highway from Auburn, Alabama, to Columbus, Georgia, with the vehicle moving at speeds of up to 105 km/h (65mph). The first road test involved one bent antenna to test the SMM case. In the second road test, all antennas worked well as a normal case for comparison with the SMM performance.

To study the effect of STBC and the number of streams on network performance, three different configurations of bent antennas were investigated as shown in Figure 5-4. STBC is a technique used in IEEE 802.11n for reducing data loss by transmitting multiple copies of the same data across several antennas to improve the reliability of data transfer since various received versions

of the data can be exploited. For STBC to function properly, the number of streams used in IEEE 802.11n networks should be carefully chosen, because one malfunctioning stream will significantly reduce the network performance. Each configuration had one pair of antennas aligned properly but not the other pair. For each of these configurations, three road tests were conducted: (1) double stream operation without STBC, (2) double stream operation with STBC, and (3) single stream operation with STBC. The network setup consists of two test platforms (with two antennas each) placed on the right side of the vehicle about 15.2 m (50 ft) apart from each other.

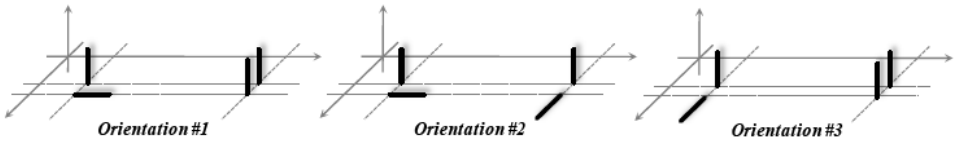

Figure 5-4. Diagram. Three Antenna Alignment Configurations for STBC and Streams Tests.

To study the performance and reliability of multi-hop packet forwarding, tests were conducted using the ad hoc network that was set up with four wireless mini-ITXs with IEEE 802.11n radios. The mini-ITXs were synchronized and the information on the number of packets transmitted per time period and the packet loss were collected, whereby the throughput and packet loss metrics were calculated. The first experiment was designed to show how throughput will decrease as the number of hops increase due to sharing of the wireless channel. The throughput was measured for one hop over 10 m (33 ft), two hops over 20 m (66 ft), and three hops over 30.5 m (100 ft). The second experiment was designed to show that throughput will decrease as the distance increases. The throughput performance was compared for 1 hop over distances of 3,6, and 30.5 m (6, 33, and 100 ft). The third experiment was designed to show that over the same distance of 30.5 m (100 ft), the throughput performance and reliability of one hop transmission is low, whereas the reliability of three hop transmission over 30.5 m (100 ft) is stable.

5.6.2 Networking Protocols for Transmission of Sensor and Actuator Control Data

For wireless transmission of the sensor data and the actuator control data between the tractor controller and the trailer sensor hub, several networking protocols and software applications are required, including TCP, IP, IEEE 802.11n MAC, CAN data bus, Universal Serial Bus (USB), and serial data bus. Since a variety of sensor types must be considered, different types of sensor communication protocols were studied. For instance, UBlox GPS uses USB, Novatel GPS uses serial bus, Oxford RT uses UDP, and string potentiometers analog/digital (A/D) converters use the CAN data bus. To transmit data from these sensors to the different sensor communication protocols over the wireless channels, there are two extreme design approaches: either collect all the sensor and control data into packets using a special software and transmit the packets or simply tunnel the sensor and control data over the wireless channels using secure shell (ssh). In

these experiments, the simpler tunnel approach was used so that the sensor data that are sent through the CAN data bus will be received over the ssh connection as CAN data at the other end of the wireless tunnel. Since ssh is connection-oriented and implemented using TCP, packet transmissions over the ssh are reliable (i.e. any packet that is dropped will automatically be retransmitted by TCP up to seven times).

In some sensors, such as Oxford RT, sensor data are transmitted over UDP packets. In this case, the UDP packets will need to be forwarded through different subnets, such as the sensor hub subnet, the wireless subnet, and the controller subnet. By using IP routing, UDP packets will be automatically routed from the sensor hub to the controller at the tractor.

TCP and UDP packets will be transmitted over IP and IEEE 802.11n MAC protocols. In order to improve the performance of these transmissions, it is important to improve the performance of the wireless IEEE 802.11n MAC layer where most of the performance degradation will occur.

5.7 Performance Results and Evaluations

5.7.1 Results of APM in Wireless Intra-vehicle Communication

APM occurs when the two antennas are not parallel to each other. Data transmission is reliable between transmitting and receiving antennas when both antennas have the same spatial orientation (i.e., have the same polarization). Otherwise, the power of wireless signal propagation between the two antennas will be reduced, causing the SNR at the receiving antenna to be reduced. Hence the data delivery ratio is reduced. Since mobile vehicular networks cannot guarantee the same (and constant) polarization between two antennas on two moving vehicles, APM will always occur, causing a reduction in the packet delivery ratio and throughput.

In the experiment to transmit GPS information wirelessly from the third trailer to the tractor, the results showed that the GPS data were transmitted correctly with no loss and at a rate of approximately 4 kbps to 6 kbps (due to the slow rate in which the GPS generated the data). This performance is possible even in the presence of APM.

Experiments were performed to measure the maximum throughput and packet loss in mobile wireless intra-vehicle networks in the presence of polarization mismatch. When the truck was stationary at the garage, and the test bandwidth was increased to 100 Mbps, the actual throughput kept increasing linearly to 100 Mbps (Figure 5-5). In a separate experiment, Figure 5-7 shows that when the truck is moving around the track, the actual throughput increased linearly as the test bandwidth is increased to 45 Mbps. (Test bandwidth is the maximum transmission rate that we set for the wireless protocol to transmit.) However, when the test bandwidth is increased further from 45 Mbps to 100 Mbps, the actual throughput fluctuated between 40 Mbps and 60 Mbps (Figure 5-6). This degradation in network performance occurred in both the straight and curved portions of the NCAT test track. This is an interesting result. Our conclusion from the analysis of these results is that when the tractor-trailer is stationary, the throughput can be

increased to 100 Mbps. However, when the tractor-trailer is moving, the maximum throughput is limited to 40 Mbps because of significant packet loss due to APM. The main reason for this appears to be that when the tractor is moving, the movements and vibration of the third trailer relative to the tractor may have caused the two stream transmission of IEEE 802.11n to fail due to APM, because only one stream is possible. This leads to the limit of 40 Mbps throughput. The packet loss is also increased to about 10% at 50 Mbps transmission rate when the truck is moving, compared to only 3% packet loss when the truck is stationary.

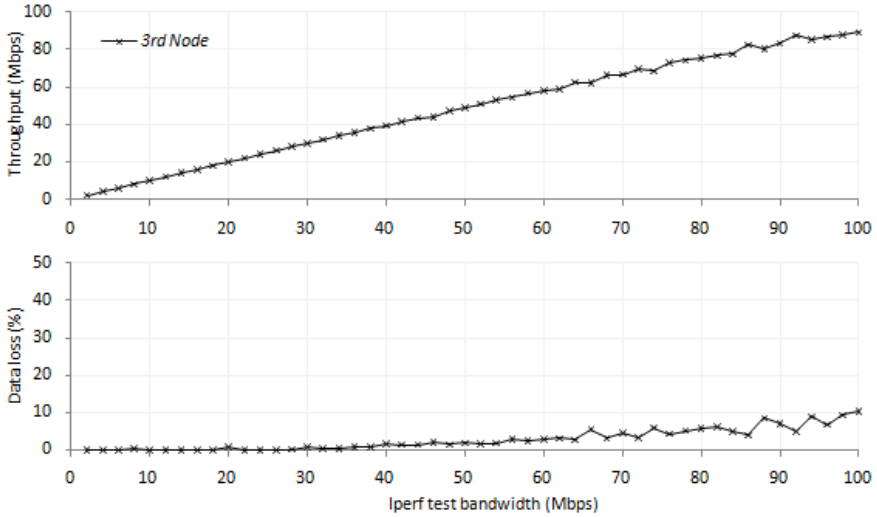

Figure 5-5. Graphs. Results of Wireless Intra-Vehicle Networks with Tractor-Trailer Stationary in NCAT Garage.

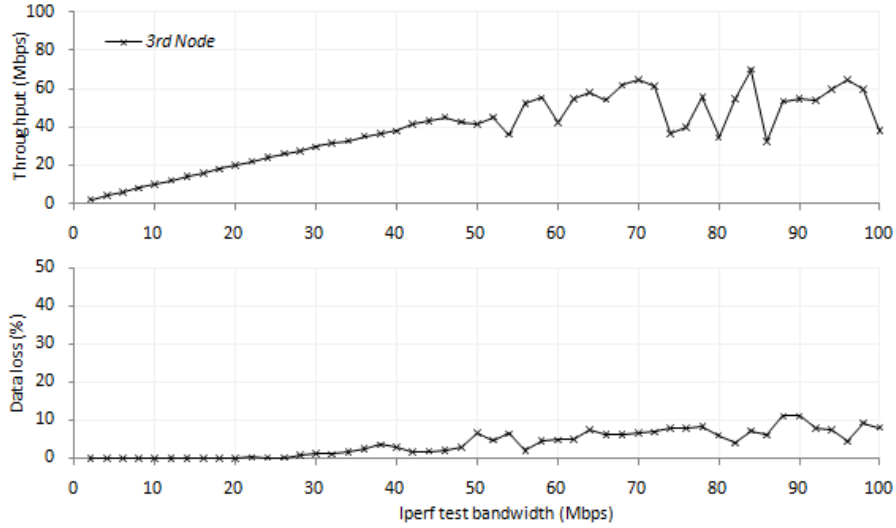

Figure 5-6. Graphs. Results of Wireless Intra-Vehicle Networks with Tractor-Trailer Running at NCAT Test Track.

5.7.2 Results of SMM

Spatial multiplexing uses simultaneous transmission from independent and separately encoded data signals (i.e., streams) through each of the multiple transmit antennas to improve throughput performance. However, spatial multiplexing will malfunction when there is a failure of some of these data streams, possibly due to problems with the transmit antennas. Since spatial multiplexing is used extensively in IEEE 802.11n to improve performance, a malfunctioning of this feature can drastically reduce the network performances.

The results of the intra-vehicle road tests shown in Figure 5-7 demonstrate some interesting phenomena. During the road tests, one of the transmitting antennas was bent by the strong winds. When that occurs, the data rates of the transmitter drop from 130 Mbps (MCS index 15) to 65 Mbps (MCS index 7), the throughput oscillates drastically, and higher data loss is observed. Modulation and Coding Scheme (MCS) index number identifies the scheme used to achieve the transmission rate. This shows that spatial multiplexing does not work well with malfunctioning antennas, so the rate adaptation algorithm in IEEE 802.11n has to select a lower data rate (MCS index 7 to 0) for the single spatial stream. Therefore, it was concluded that the rate adaptation algorithm in our IEEE 802.11n platforms does not work well in the SMM situation. That means a new rate adaptation algorithm is needed for IEEE 802.11n to deal with the SMM issue.

The results in Figure 5-8 also show that in both static test and road test, when the antennas are aligned properly, good network performance can be achieved in terms of high throughput, low data loss, and stable transmission data rate. Therefore, spatial multiplexing in IEEE 802.11n requires properly aligned antennas, which are not possible in typical wireless vehicle networks. Furthermore, weather changes and unstable power supplies in vehicle networks may cause asymmetrical antenna performance, which could cause further degradation in throughput and network reliability. This means that the ESC system must be supported by wireless networks even with degraded performance, or the performance of wireless networks must be improved using advanced techniques that are investigated in this research work.

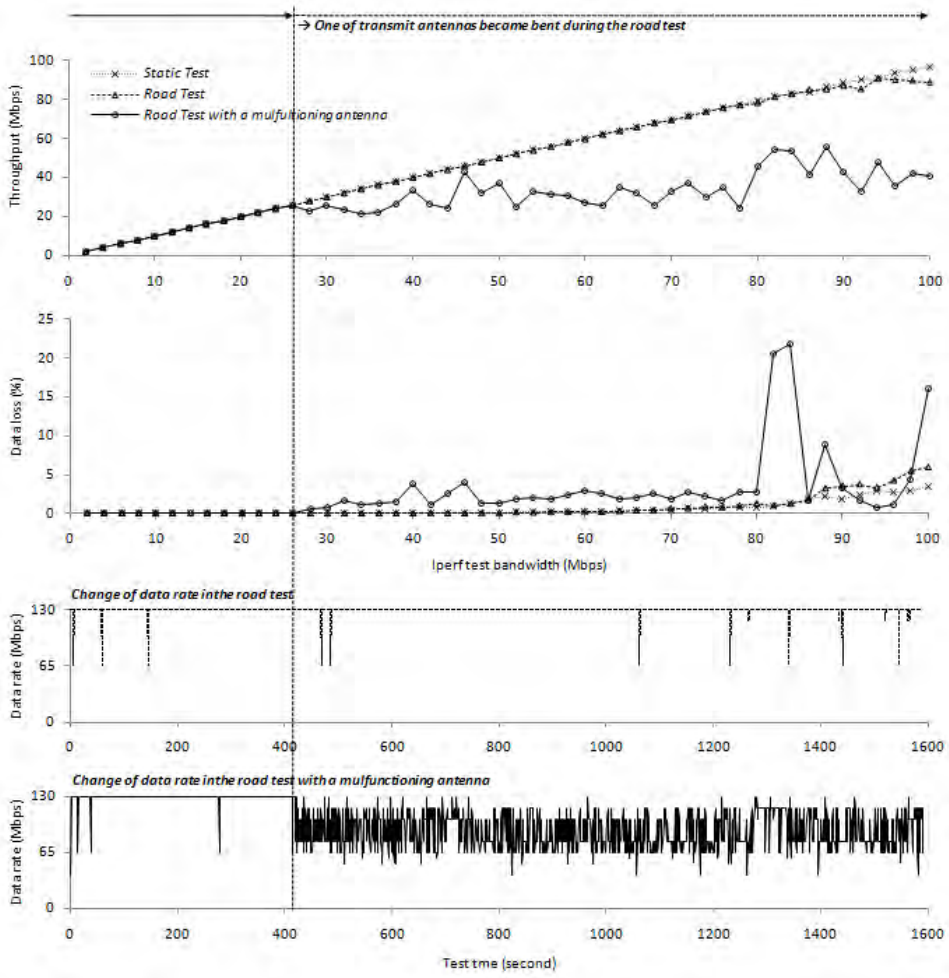

Figure 5-7. Plot. Results of Throughput and Packet Loss with SMM.

5.7.3 Results of STBC and the Number of Streams

Figure 5-8 shows road test results of throughput, packet loss, and data rates for Orientation #1, as shown in Figure 5-4. Results for other orientations are similar and are omitted for brevity. The figure depicts the throughput, data loss, and changes of data rate for three scenarios: double stream operation without STBC, double stream operation with STBC, and single stream operation with STBC. The double stream operation without STBC does not work well because of the SMM issue as is described in the previous section. Similar network performance can be found for the double stream operation with STBC due to the bent antenna. Interestingly, the single stream operation gives the best network throughput results.

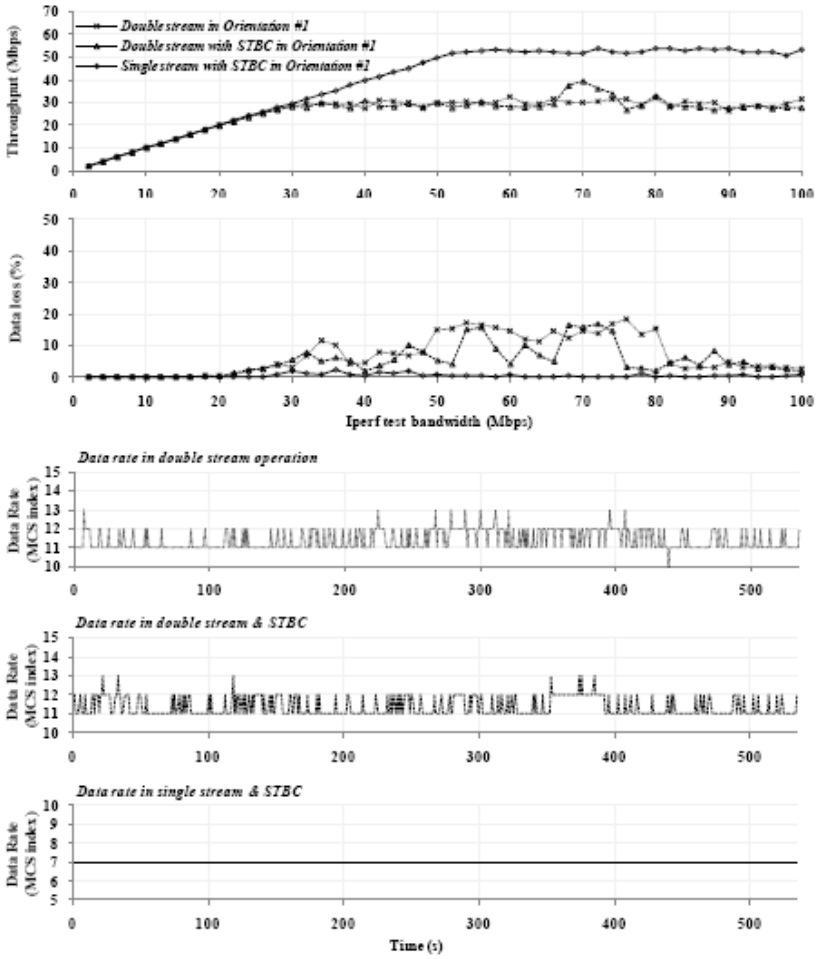

Figure 5-8. Plot. Results of Tests on Effects of STBC and Number of Streams.

The results in Figure 5-8 also show that the rate adaptation mechanism provided by IEEE 802.11n does not work properly in these experiments. This is because even though single stream operation can effectively solve the problem caused by poor antenna alignment, the current rate adaptation algorithm of IEEE 802.11n is not aware of this antenna alignment problem. Instead it assumes that the problem is due to channel fading and tries to correct the problem using an ineffective technique of reducing the data rates. In fact, IEEE 802.11n tries data rates from MCS index 13 to 11 for the double stream operations. Figure 5-8 shows a very high frequency of data rate changes in the double stream with the STBC case compared to pure double stream without STBC. However, the data rate of single stream with STBC does not change at all and remains constant at MCS index 7 because this stream uses the pair of antennas that are properly aligned. This is the main reason that the single stream gives the highest throughput performance compared to both of the two-stream cases.

Hence, single stream operation provides more reliable networks with improperly aligned antennas. Also, the optional STBC function of IEEE 802.11n helps in improving the network

stability even for the string stream transmission. These test results show that performance of wireless intra-vehicle networks will be improved for ESC if single stream with STBC is used in the IEEE 802.11n network.

5.7.4 Results of Performance of Multi-Hop Wireless Protocol

The results of the throughput tests of multi-hop packet forwarding are shown in Figure 5-9, where the maximum throughput of 1 hop over 10 m (33 ft) distance is 14 Mbps, that of 2 hops over 20 m (66 ft) is 7 Mbps, and that of 3 hops over 30.5 m (100 ft) is 5 Mbps. In the 3 hop test, this result shows that the bandwidth is shared among the three links equally, whereby the maximum throughput of 14 Mbps for the 1 hop transmission is split into three wireless channels, each with 5 Mbps. The packet loss rate is 0 in these tests. In 3 hop forwarding, the packet loss can be reduced since the distance in each hop is considerably shorter than the distance covered by a single hop. In supporting ESC applications, the reliability provided by transmission over the shorter distance in each hop will ensure that the important sensor and actuator control information is transmitted reliably (i.e. with very low loss rate).

To show the reduction in performance over longer distances, the test results in Figure 5-10 show that as the distance of one hop increases from 3 m (6 ft) to 30.5 m (100 ft), the throughput performance drops from 15 Mbps to 11 Mbps. This shows that as the distance between the hops increases, packet loss will increase and throughput will decrease. Hence for long distance transmission, it is more reliable to transmit the packet over multiple numbers of hops, each covering a shorter distance.

Regarding throughput degradation for 1 hop over a large distance, the test results in Figure 5-11 show that for 1 hop over 30.5 m (100 ft), the throughput is reduced to 11 Mbps (instead of 14 Mbps over 10 m (33 ft) distance), whereas the throughput for 3 hops over 30.5 m (100 ft) remains the same at 5 Mbps.

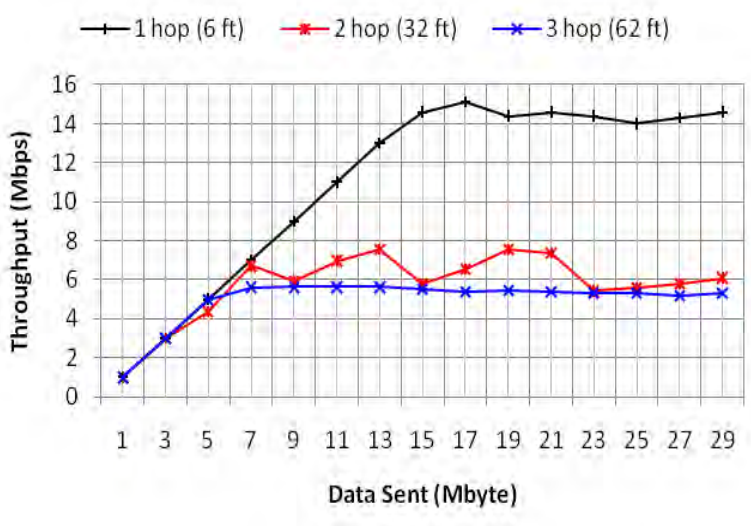

Figure 5-9. Plot. Results of Throughput Tests of Multi-Hop Packet Forwarding.

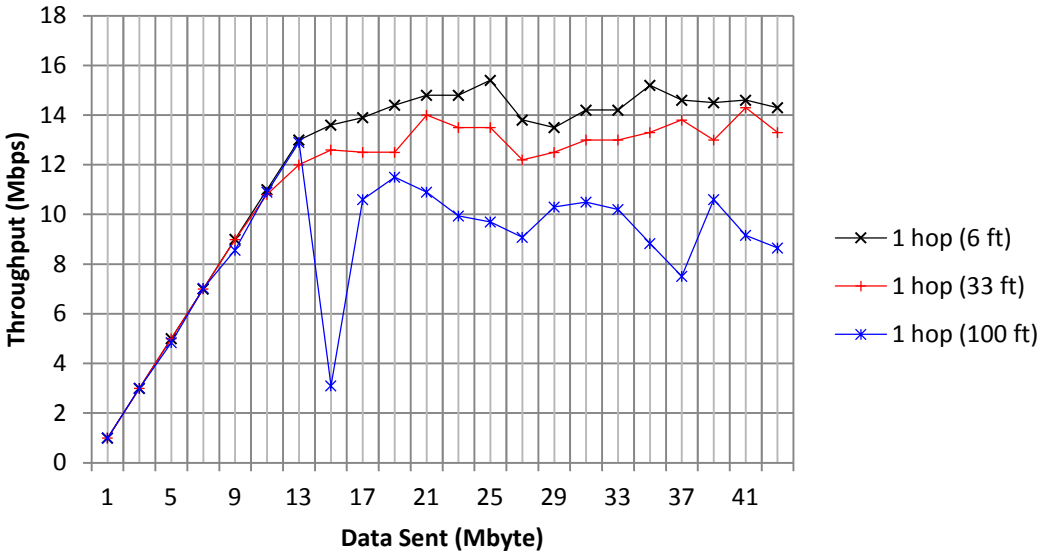

Figure 5-10. Plot. Results of Throughput Tests for Different Distances in Each Hop.

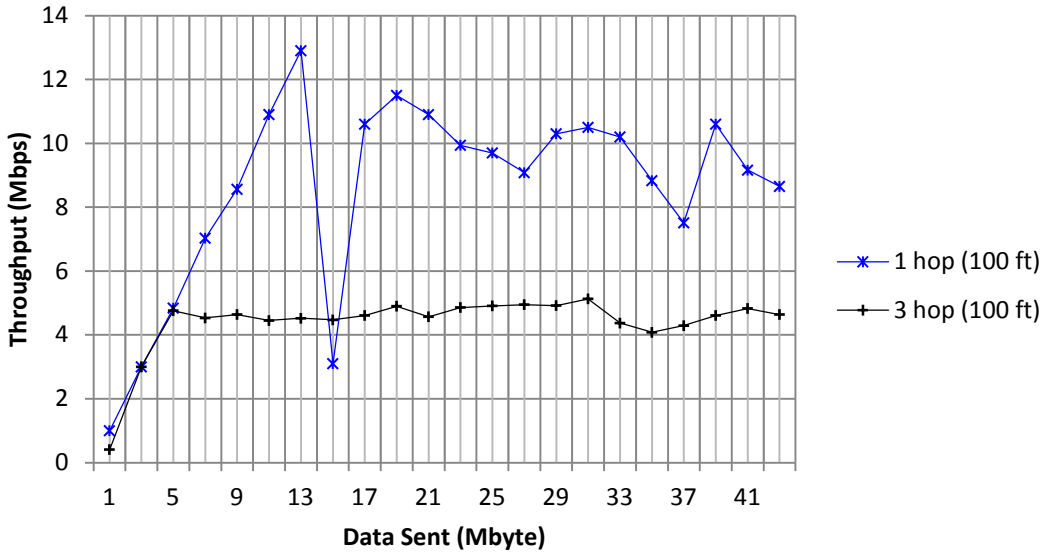

Figure 5-11. Plot. Results of Throughput Tests for Different Number of Hops over the Same Distances.

The results of the multi-hop experiment are summarized in Table 5-1. The majority of the values are obtained from the experiments and some values are obtained by interpolation.

Table 5-1. Maximum throughput rate achieved at different distances in the multi-hop experiments.

Number of Hops	Distance			
	2 m (6 ft)	10 m 33 ft	20 m 66 ft	30.5 m 100 ft
1	15 Mbps	14 Mbps	13 Mbps	12 Mbps
2	9 Mbps	8 Mbps	7 Mbps	6 Mbps
3	6 Mbps	5 Mbps	5 Mbps	5 Mbps

5.7.5 Results of Performance of Efficient Broadcast Protocol

The performance and reliability of the efficient broadcast protocol is measured by its throughput, and delivery ratio. Figure 5-12 shows the comparison of throughput between traditional broadcast and efficient broadcast with aggregation. Intuitively, throughput is proportional to the number of nodes; however, in traditional broadcast, the increased number of nodes may interrupt transmissions due to the flooded data packets. Therefore, in traditional broadcast, throughput significantly degrades as the number of nodes increase. On the other hand, efficient broadcast with aggregation does not increase the number of packets and hence throughput actually increases as the number of nodes increase.

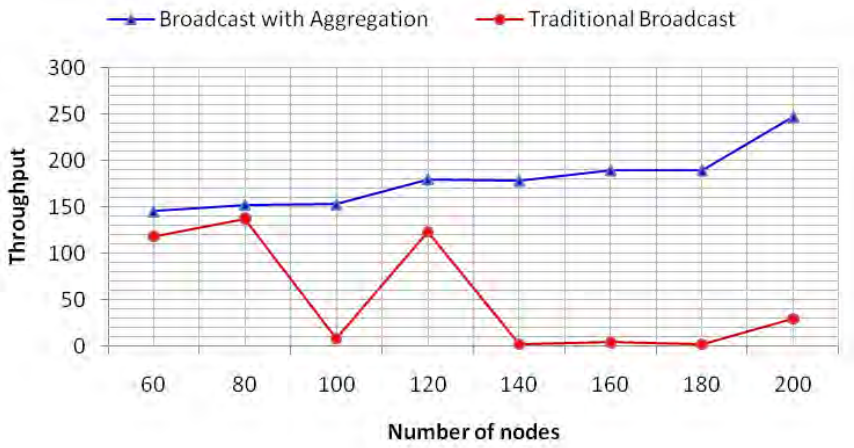

Figure 5-12. Graph. Throughput for Broadcast with Aggregation and Traditional Broadcast.

Delivery ratio is defined as the number of packets received at the destination divided by the number of packets transmitted. As can be seen in Figure 5-13, traditional broadcast shows a very unstable rate as the number of nodes changes, whereas in the case of efficient broadcast with aggregation, the delivery ratio remains constant as the number of nodes increases.

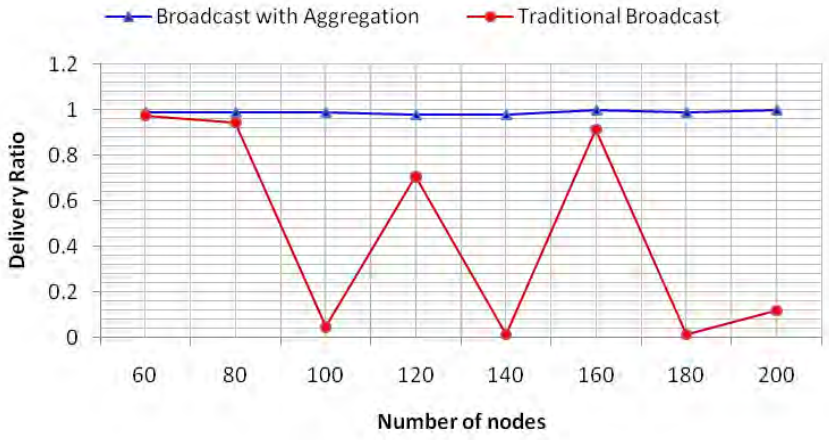

Figure 5-13. Graph. Delivery Ratio for Efficient Broadcast with Aggregation and Traditional Broadcast.

This page intentionally left blank.

Chapter 6 – High Throughput Wireless Vehicle Networks

6.1 Performance Degradation Problems in Wireless Vehicle Networks

Because of the harsh operating environments of commercial vehicle wireless networks, performance of wireless transmission may degrade mainly due to channel fading, interference, mobility, APM, vibration, data packet collision, and jamming. The performance degradation problem was considered to be less severe than the reliability problem discussed in Chapter 5 because even when performance degrades, transmission is still possible although at a lower data rate, whereas in reliability problems the degradation is often too severe that transmission may be impossible. In these cases, techniques were considered to improve performance when the wireless conditions will degrade performance so that the data rate under those circumstances could be maximized.

6.2 Techniques for Improving Throughput of Wireless Vehicle Networks

6.2.1 Optimizing Antenna Orientation for Improving Throughput

The alignment of antennas plays an important role in determining the maximum data rate that can be achieved in a wireless transmission. The optimal antenna orientation needed to be determined that will maximize the throughput performance, particularly in mobile commercial vehicles where motion and vibration can cause degradation in the throughput performance. The optimal antenna alignment should cover as many different orientations as possible. Since only two antennas were used for IEEE 802.11n, the two antennas should then cover orthogonal direction (i.e. should be perpendicular to each other). These antenna alignments are designed to overcome the problems of APM and SMM in wireless vehicle networks. Three different alignment configurations tested are shown in Figure 6-1, with Orientation #3 being the configuration that covers orthogonal directions.

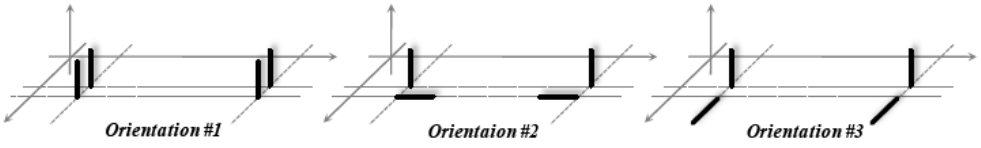

Figure 6-1. Diagram. Three Antenna Alignment Configurations for Optimal Antenna Alignment Tests.

6.2.2 Fast Recovery Transmission Rate Adaptation Method

The second method for improving throughput and reliability is using a FRRA algorithm. This uses small probe packets to accurately determine whether the cause of poor transmission throughput is fading or interference. If the cause is fading, then the transmission rate is reduced in order to improve the delivery ratio (i.e. reduce packet error rate) thus improving the vehicular network robustness and throughput. Since wireless conditions may change frequently, this algorithm provides fast recovery when the dominant problem changes from fading to

interference, in which case the algorithm will switch to methods for avoiding interference and maintaining high transmission rate. The effect of FRRA rapid reaction to the changing wireless conditions will allow FRRA to improve the throughput and reliability of intra-vehicle wireless networks.

6.2.3 Dynamic Channel Hopping Method

The Dynamic channel hopping method was discussed in Section 4.5 in the context of overcoming jamming attacks. However, in some cases, interferences can occur in the form of benign transmission of devices that could be communicating among themselves independently and are unaware that they are causing interference. In such cases, dynamic channel hopping will be useful for overcoming these types of interferences. As before, both proactive and reactive channel hopping may be used. In the case of proactive channel hopping, the wireless devices continually switch channel, whether there is interference or not. In reactive channel hopping, the wireless device will switch channels only if interference is detected by computing the channel utilization value. Comparing both proactive and reactive, it is more appropriate to use reactive channel hopping to overcome benign interference because the interference does not try to track the channel of the communicating users, but instead stay in that particular channel. In jamming attacks, the attacker could track the channel in current use and jam that channel. The results and analysis of the performance of dynamic channel hopping is discussed in Section 4.6.

6.3 Implementation of Efficient Rate Adaptation Algorithm

The FRRA algorithm was implemented in the ““ath9k”” driver for IEEE 802.11n executing first on the Fedora14 Linux Operating System and later revised for Fedora15 with compatible wireless version 2.6.38.2-2. The implementation contains codes for measuring and analyzing performance of the protocol.

One of the main issues that was encountered in IEEE 802.11n wireless transmission is a tendency for a large number of frame errors, which can be corrected using retransmissions through the proper automatic request response protocol. However, setting the right retransmission limit becomes important. At first, the retransmission limit, in other words, Multi-Rate Retry (MRR), is set to 4. This means that if FRRA fails to transmit a frame after trying 4 times at the same rate, then FRRA abandons the frame. In this case, when the MRR is set at 4, experience shows that the protocol will drop many frames. However, when the MRR is set at 20 (r0:8 r1:4 r2:4 r3:4), then the number of dropped frame is very much reduced. The MRR notation of (r0:8 r1:4 r2:4 r3:4) means that when a frame transmission fails, the protocol will retry transmission first at rate “r0” for another 7 times, for a total of 8 tries, and if those fail, it will then retry transmission at a lower rate of “r1” for 4 times. If those fail, it will retry transmission at a lower rate “r2” for 4 times and if those fail, it will retry transmission at a lower rate of “r3” for another 4 times. If all those fail, then the frame will be dropped; otherwise the frame is

transmitted successfully. This MRR setting is the same as used in the “ath9k” rate adaptation and in Minstrel.

6.4 Experimentations and Simulations

To study the effect of different antenna alignment on network performance, experiments were conducted with three different alignment configurations as shown in Figure 6-1. These antenna alignments are designed to overcome the problems of APM and SMM in wireless intra-vehicle networks. In these experiments, the antenna alignment needed to maximize wireless network throughput was investigated. These antenna alignment tests were conducted using two test platforms (with two antennas in each platform), separated by a distance of 15.2 m (50ft) from each other. The road tests were also conducted on the I-85 highway from Auburn, Alabama, to Columbus, Georgia, with the vehicle moving at speeds of up to 104.6 km/h (65mph).

To study the performance of the FRRA algorithm, two set of tests were conducted, stationary and mobile, to measure the performance of FRRA, “ath9k”, and Fixed-Rate (fixed at 117 Mbps) algorithms. The “ath9k” protocol uses its own rate adaptation algorithm. The distance between the sending and receiving antennas is fixed at 3 m (10ft). The test was conducted using test bandwidth from 31 Mbps to 99 Mbps at 3 Mbps intervals. The loss rate is averaged throughout all the experiments.

6.5 Performance Results and Evaluations

6.5.1 Results of Optimal Antenna Orientation

Previous experimental results have provided better insights into the problems of APM and SMM in wireless intra-vehicle networks. Based on these new insights, methods were investigated to overcome these problems by conducting further experiments to investigate the antenna alignment needed to maximize wireless network throughput. The difference between optimal antenna alignment and avoiding polarization mismatch is that when the truck is moving, then polarization mismatch cannot be avoided; hence the maximum throughput can be obtained only using Orientation #3 in Figure 6-1. Although it is very difficult to implement antennas that are perfectly aligned all the time in real vehicle networks, it is still important to understand the optimal antenna alignment that gives the best network performance, which can take advantage of spatial multiplexing and rate adaptation algorithms.

Outdoor antenna alignments are more important than indoor antennas because in indoor environments, IEEE 802.11n may use multi-path signal reflections from building walls. On the other hand, in a typical (outdoor) vehicular network on the roads or highways, there are usually insufficient multi-path signals.

From the experiment results shown in Figure 6-2, the antenna configuration of Orientation #3 gives the antenna alignment that provides the maximum network throughput. In this

configuration, there is one pair of vertical antennas and another pair of horizontal antennas, described as follows.

The main technique used by IEEE 802.11n to achieve a high throughput is spatial multiplexing, which allows data to be split and transmitted via independent data streams from different antennas. The best antenna alignments would be those that are most effective in achieving maximal spatial multiplexing in IEEE 802.11n. Three antenna configurations were designed to achieve this, as shown in Figure 6-1. The results in Figure 6-2 show the best antenna configuration. Orientation #1 uses parallel alignment of all antennas, which is considered the basic setting for WiFi antennas. Orientations #2 and #3 are better antenna alignments that may provide the optimal alignment, since they cover both vertical and horizontal orientations.

The test results in Figure 6-2 show the throughput, data loss, and changes of data rate for each of the three examples discussed above. Orientation #1, the basic IEEE 802.11n antenna alignment, does not work well because it covers only one antenna polarization. Interestingly, Orientation #3 gives the best network performance in terms of higher throughput, lower data loss, and stable data rate during the test. This configuration effectively uses orthogonal spatial streams to deliver data, so signals on both vertical and horizontal polarizations are well covered. Although the antenna alignment in Orientation #2 is similar to Orientation #3, its performance is worse than Orientation #3 because the signals on the horizontal polarization are weaker in that orientation.

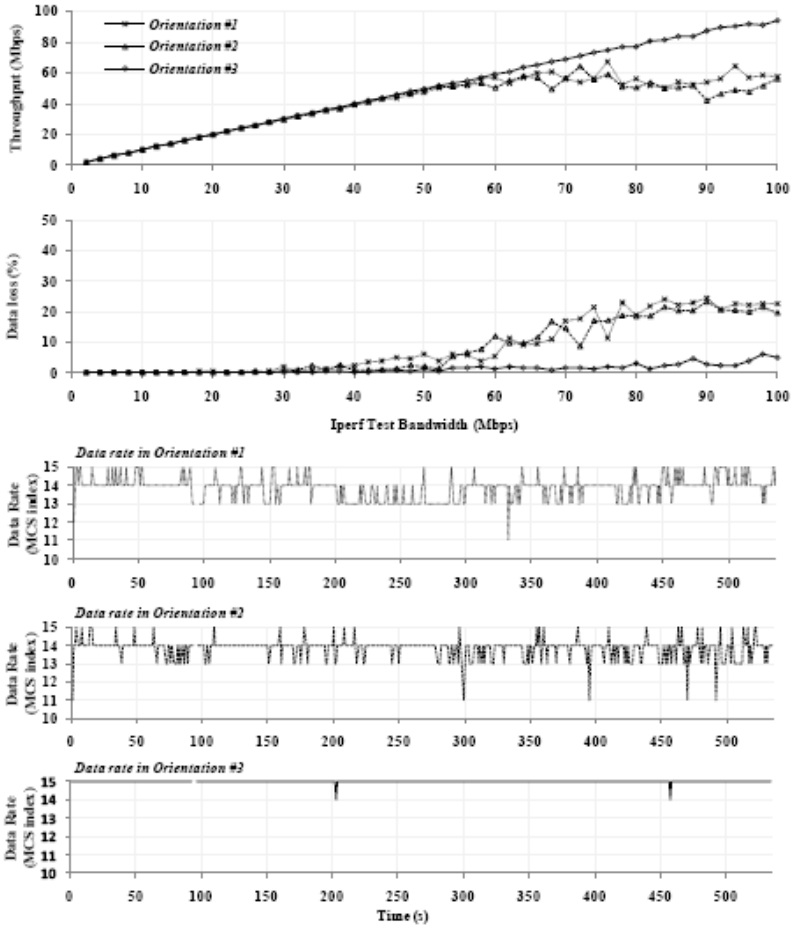

Figure 6-2. Graphs. Results of Tests on Optimal Antenna Alignments.

These experimental results show that antenna-polarization diversity is critical for supporting spatial multiplexing more effectively and thus results in higher data rates and greater reliability compared to a system with only one single polarization. Therefore, IEEE 802.11n technology should consider the antenna polarization effect to fully utilize its functionality and maximize its performance and reliability for wireless intra-vehicular networks.

6.5.2 Results of Throughput Performance of FRRA Algorithm

The results of the stationary tests with the FRRA algorithm in Figure 6-3 show that FRRA gives a slightly better performance and lower loss rate than “ath9k” and fixed rate (117 Mbps). FRRA performs slightly better for all test bandwidths from 31 to 99 Mbps. FRRA particularly performs better than the “ath9k” rate adaptation algorithm for test bandwidths from 85 Mbps to 99 Mbps.

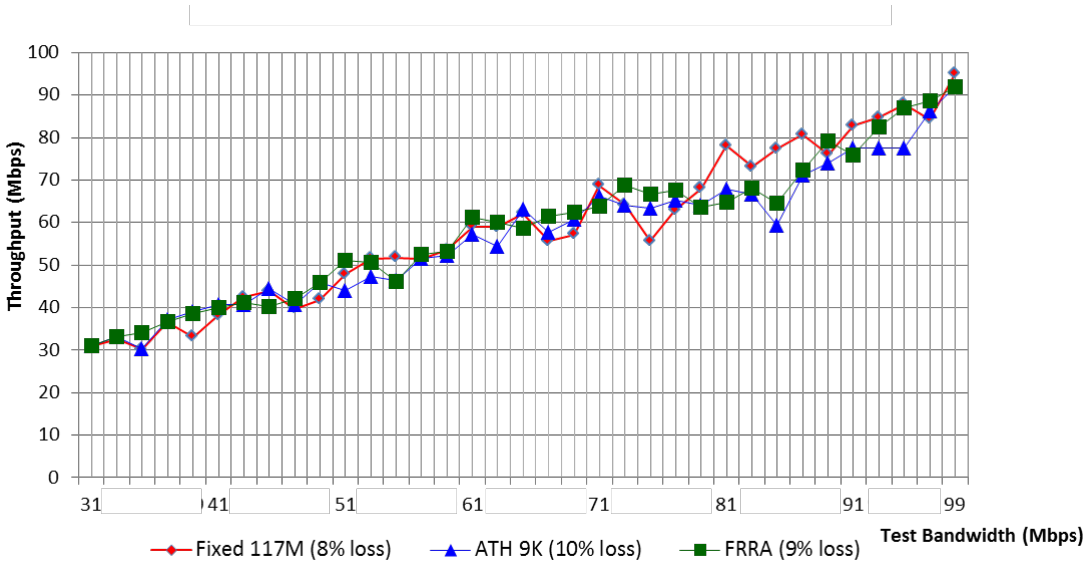

Figure 6-3. Graph. Results of Stationary Tests of Fixed Rate, "ath9k", and FRRA Algorithms.

The results of the mobile tests at 32.2 km/h (20 mph) with the FRRA algorithm in Figure 6-4 show that FRRA still gives a slightly better performance and lower loss rate than "ath9k" and fixed rate (117 Mbps) for test bandwidths from 31 to 81 Mbps. However, from 85 Mbps to 91 Mbps, FRRA performs worse than the other protocols. This can be attributed to the behavior of FRRA, which respond too aggressively to channel quality variation and thus adversely affect the throughput. In future work, it should be investigated how to improve FRRA further by using more advanced techniques, particularly for addressing the problems of spatial multiplexing that were discussed in the previous set of experiments. Future work will include more tests on FRRA to demonstrate that since FRRA can distinguish between collisions and channel fading, it will better handle large variations in the actual vehicle networking environments that may cause excessive collisions and channel fading.

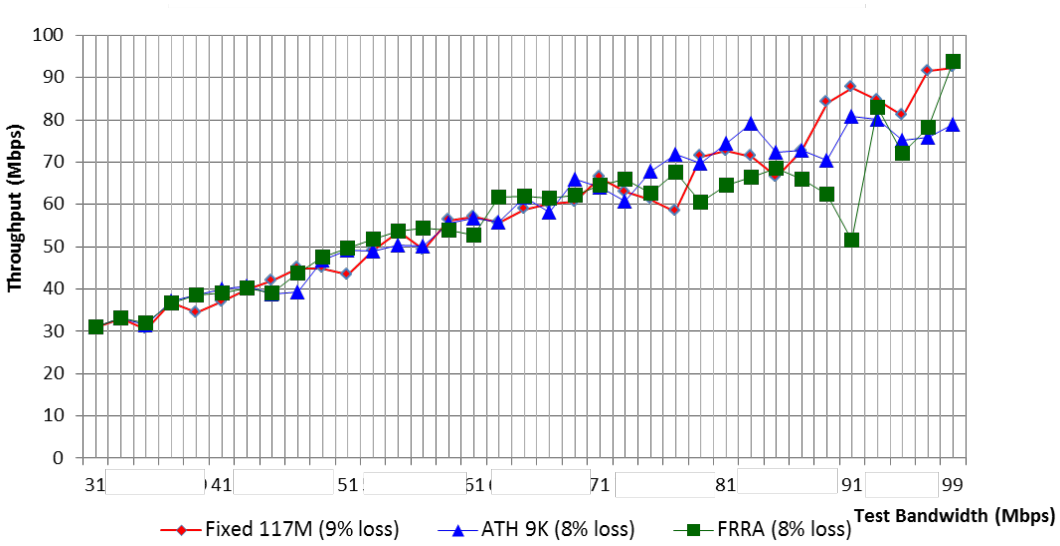

Figure 6-4. Plot. Results of Mobile Tests of Fixed Rate, “ath9k”, and FRRA Algorithms.

This page intentionally left blank.

Chapter 7 – Precise Vehicle Positioning

7.1 Dynamic base Real-Time Kinematic (DRTK) Systems

A DRTK system is a technique for drastically improving the GPS position solutions for a moving receiver. This technique was implemented in ESC. This is a multi-stage process that incorporates the techniques and algorithms of Differential GPS (DGPS) and standard Real-Time Kinematic (RTK) systems. The "normal" GPS position solutions have several errors that delay the signal, and GPS receivers derive position solutions based on time alone. These errors include the atmospheric errors from the signal being refracted as it goes through the ionosphere and troposphere, multi-path errors as the signal is relayed off of the surrounding environment, as well as the internal clock bias errors in both the satellites and the receiver. These errors are affected by several variables; primarily the satellite constellation configuration as well as the satellite elevation angles, which affect the ionospheric error more as the satellites are lower on the horizon as the signal has to travel through more of the atmosphere.

7.2 Global Position System Signals

GPS satellites send out their signals at several frequencies. The L1 band is sent at a frequency of 1,575.42 MHz with a wavelength of 19.05 cm, this is the Coarse-Acquisition (C/A) code and is open to be used by the public. The L2 band is sent at a frequency of 1,227.60 MHz with a wavelength of 24.45 cm, this is the P(Y) code and is available only for military applications as this code requires to be encrypted. The military intentionally degrades the integrity of the L1 frequency by adding errors into it to limit the accuracy. This is called Selective Availability (SA) and its purpose is to prevent any U.S. enemy from using our own GPS signals against us. Without the code to encrypt the L2 signal, the accuracy of the position is based solely upon the L1 signal; this accuracy depends on the errors mentioned above, but can usually be assumed to be between 5-10 m. However, the industry has figured out a way to get around this intentionally degraded signal to achieve precise positioning solutions, this technique is called Differential GPS (DGPS).

7.3 Differential GPS

Differential GPS solutions can bring the error down from meters to centimeters, sometimes under 10 cm position error is possible depending on the scenario. When GPS receivers are operating within a close proximity (Figure 7-1), usually assumed to be under 10 km, the errors from the atmosphere are highly correlated and DPGS techniques can mitigate these common errors.

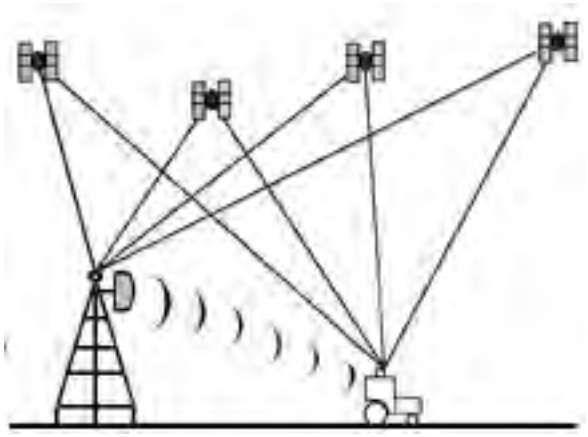

Figure 7-1. Diagram. Differential GPS Technique.

DGPS methods can either use the pseudorange measurement, the carrier phase measurement, or both. The pseudorange is the true range plus all of the errors. The carrier phase measurement is the number of the GPS signal cycles that have been accumulated since the time of the signal acquisition. Using the carrier phase measurement can lead to a much more precise solution than when using the pseudorange alone, but this ambiguous number of accumulated cycles needs to be estimated accurately. The issue in estimating this integer ambiguity is the sinusoidal signal is off by one, which would result in a 19 cm error. When this carrier phase integer ambiguity is accurately estimated, the Relative Position Vector (RPV) can be estimated on the order of a couple of centimeters. RTK systems exploit the accuracy of the carrier phase integer ambiguity measurement.

7.4 Real-Time Kinematic (RTK) Systems

In a RTK system, a static base station with known GPS coordinates is used to communicate its location to a dynamic receiver operating in close proximity. In this project, the static base station was located on the hill by the track and the dynamic receiver was the triple tractor-trailer. For RTK systems to work, they need to be in constant communication with the dynamic receiver. This was accomplished by using a radio modem. Because the radio modem uses the UHF band, it requires line-of-sight with the base station. A technique that can also be exploited is the use of a dynamic base station as opposed to the static base station that RTK uses. This technique is called DRTK.

7.5 Implementation in this Project

In this project, the tractor and second trailer were the dynamic bases that were in communication with the static base station. In a DRTK system, the global positioning is lost, but the relative positioning vector is maintained to centimeter accuracy. The radio modems were placed on top of the tractor and second trailer and the RPV to both the first and third trailers could be calculated.

Finding the RPV is a multi-step process. First, the process of Single Differencing (SD) is implemented, which is the process of taking the measurement differences between the base station and receiver to one of the satellites. With the SD calculated, the next step is to find the Double Differences (DD), which is the SD of the receivers to each of the visible satellites in the pseudorange and carrier phase measurements.

After the DD is calculated, the RPV is estimated through another multistep process. This includes using the Kalman filter to give a floating point estimate of the carrier phase integer ambiguity, implementing the LAMBDA method to fix the ambiguous integer, and using the Least Squares method to estimate the RPV.

This project also showed that ESC allowed for the implementation of all of these techniques. For the DRTK to be run real-time, it not only required the constant radio communication to the static base station, but also the constant communication between each of the receivers on the tractor and trailers. In the LCV testing, the data was sent via a CAN bus that ran the length of the vehicle combination. In the ESC testing, the data was sent from each of the GPS receivers wirelessly up to the central computer at the tractor via wireless modems and routers.

Being able to send the data wirelessly is a much more convenient, and potentially more effective, means of communication and when combined with the implementation of a DRTK system, can lead to a much more effective ESC for tractor-trailers.

This page intentionally left blank.

Chapter 8 – Conclusions

The results of this project on the integrated wireless vehicle networks for V2V, V2I and intra-vehicle networks show that the integrated network can satisfy the security, reliability and throughput performance requirements of ESC systems and other connected vehicle safety applications. The demonstration of the intra-vehicle wireless networks on the commercial tractor trailers at the NCAT test track showed that this is feasible in real-world vehicle networks under normal operating conditions.

8.1 Satisfying the Requirements for Intra-Vehicle Wireless Communication

The experimental results with IEEE 802.11n wireless transmission show that a minimum of 20 Mbps throughput can be achieved even in the presence of wireless transmission problems, such as polarization mismatch and SMM. The test results also show that packet loss rate is limited to no more than 10%. IT was also shown that the total throughput requirements of ESC applications, for both the sensor and control data, is 158.4 kbps, even after taking into account 10% packet loss rate. This shows that IEEE 802.11n links can be used to satisfy the communication requirements of intra-vehicle wireless networks for supporting ESC applications.

With further improvements in the IEEE 802.11n MAC protocols, such as using more advanced rate adaptation protocols, multi-hop packet forwarding, and efficient broadcasting, the throughput performance and reliability of wireless links can be improved further to ensure that intra-vehicle wireless networks support ESC systems at a higher level of confidence.

8.2 Selection of Wireless Communication Protocols

IEEE 802.11n was selected for implementing intra-vehicle wireless networks because of the various performance enhancing techniques used in this protocol. The techniques which provide the highest throughput (up to 300 Mbps), such as MIMO, spatial multiplexing, MCS, STBC, and channel bonding were investigated. Even in harsh outdoor vehicle networking environments it was discovered that throughput and packet loss rate performance is adequate for supporting ESC. This conclusion remains true even in the presence of wireless transmission problems that were have studied, such as polarization mismatch and SMM.

In comparison, the throughput of DSRC radios, such as Kapsch DSRC radios, is only about 3 Mbps. Because IEEE 802.11n provides significantly higher throughput than DSRC radio, it is appropriate to use them for implementing intra-vehicle wireless networks. Despite this, since DSRC is designated for V2V and V2I communication, there is a need for DSRC to be used for inter-vehicle communication. However, it is feasible to maintain two vehicle wireless networks: (1) IEEE 802.11n for intra-vehicle communication and (2) DSRC for V2V and V2I communications.

This page intentionally left blank.

Chapter 9 – Further Research

In order for these novel wireless vehicle network protocols and techniques to be deployed and support commercial connected vehicles research further tests are needed on the performance, reliability, security and feasibility of practical wireless devices that can be installed on the commercial tractor-trailer. Continued work should keep reducing the size and cost of the wireless devices that will still meet the throughput and reliability requirements of ESC systems and safety applications. More tests will need to be conducted to evaluate the performance and reliability of the protocols under more hazardous wireless conditions, such as heavy rain, fog or snow. Wireless protocols should be designed specifically to overcome these adverse weather conditions.

9.1 Chapter Overview

The integrated wireless vehicle networks for supporting V2V, V2I and intra-vehicle networks needs to show that they will satisfy the security, performance, and reliability requirements of actual vehicle safety applications and ESC in commercial tractor semi-trailers. More studies need to be done to demonstrate that this goal can be achieved under real-world road and highway conditions and using actual commercial tractor semi-trailers. The studies on these real vehicle network systems operating under real-world wireless conditions will construct an understanding of the behavior of the network protocols. These insights will enable the further improvement on wireless network protocols for overcoming any performance degradation and develop more advanced techniques to ensure security, reliability and throughput performance of the protocols under these real-world environments.

9.2 Supplemental Ideas and Future Work

For the integrated wireless vehicle network to be deployed in real commercial vehicles in the actual road and highway conditions, further improvement of protocols to provide higher reliability and throughput is needed. More efficient techniques should be developed dynamic clustering for dynamic channel allocation and security management. Security of wireless vehicle networks should be improved to avoid potential security loop-holes and problems in the implementation of IEEE 802.11i authentication and key management. To avoid jamming, better countermeasure techniques should be developed that will also provide high throughput and reliability. More advanced protocols and techniques should be developed to improve wireless network reliability, which could be based on variations of multi-hop packet forwarding and efficient broadcast mechanisms. To improve data rate and reliability further, other rate adaptation algorithms should be developed that will also improve on its accuracy in distinguished channel fading from data packet collision. Precise vehicle positioning may further be improved using the current data collections and analysis to design more accurate and reliable GPS based relative positioning in tractor-trailers.

In the intra-vehicle networks research, although the experimental studies and requirement analysis show that IEEE 802.11n can satisfy the requirements for wireless ESC systems, there is still a need to further investigate the actual implementation of wireless networking for vehicle safety applications and ESC in tractor-trailer environments. In intra-vehicle wireless network systems, protocols for ESC should be designed, and actual performance results measured and analyzed. In V2V and V2I communications, protocols should be designed that will improve the reliability and throughput for some typical vehicle safety applications. The actual performance results can then be compared to the design analysis and the outcome be used to enhance the design and implementation in order to improve performance.

9.3 Conclusions

Integrated vehicle networks that support V2V, V2I and intra-vehicle networks in commercial vehicles are beneficial for supporting many vehicle safety and mobility applications. Intra-vehicle wireless communication provides many benefits in supporting vehicle stability control systems where the sensor and actuator control data are transmitted wireless between the tractor and trailers. V2V communication can provide benefits in sending critical safety information from one vehicle to another, thus avoiding potential accidents. V2I wireless networks can provide benefits in communicating important road, traffic, terrain, or weather information. More research is required to develop the techniques, protocols and algorithms for integrated vehicle wireless networks that can satisfy the security, reliability and throughput performance requirements of ESC systems and other connected vehicle safety applications.

Chapter 10 – References

Abraham, S., Meylan, A., and Nanda, S. 2005. 802.11n MAC design and system performance. In: IEEE International Conference on Communications, 2005,vol 5, pp 2957–2961.

Achanta, M., 2006. Method and Apparatus for Least Congested Channel Scan for Wireless Access Point, *US Patent No. 20060072602*. Apr. 2006.

ACS 2011. http://wireless.kernel.org/en/users/Documentation/acs

Alnifie, G., and R. Simon, 2010. MULEPRO: a multi-channel response to jamming attacks in wireless sensor networks, *Wireless Communications and Mobile Computing*, vol. 10, no. 5, pp. 704–721, May 2010.

ASTM International. 2003. Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems – 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications; ASTM E2213-03.

Balasubramanian, A., Mahajan, R., Venkataramani, A., Levine, B.N., Zahorjan, J. 2008. Interactive wifi connectivity for moving vehicles. In: Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication, 2008, pp 427–438.

Broustis, I., K. Pelechrinis, D. Syrivelis, S. V. Krishnamurthy, and L. Tassiulas, 2009. FIJI: Fighting implicit jamming in 802.11 WLANs, *Security and Privacy in Communication Networks*, vol. 19, pp. 21–40, Oct. 2009.

Bychkovsky, V., Hull, B., Miu, A., Balakrishnan, H., Madden, S. 2006. A measurement study of vehicular internet access using in situ Wi-Fi networks. In: Proceedings of the 12th Annual International Conference on Mobile Computing and Networking, pp 50–61.

Cheng, L., Henty, B.E., Stancil, D.D., Bai, F., and Mudalige, P. 2007 Mobile Vehile-to-Vehicle Narrow-Band Channel Measuremnet and Charaterization of the 5.9 GHz Dedicated Short Range Communication (DSRC) Frequency Band. In: IEEE Journal on Selected Areas in Communications 25(8): 1501–1516.

Eriksson, J., Balakrishnan, H., and Madden, S. 2008. Cabernet: Vehicular content delivery using WiFi. In: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, 2008, pp 199–210.

Ervin, R.D., Fancher, P.S., and Gillespie, T. 1984. An Overview of the Dynamic Performance Properties of Long Truck Combinations. UMTRI-84-26, University of Michigan (UMTRI).

Ferreri, F., M. Bernaschi and L. Valcamonici, 2004. Access points vulnerabilities to DoS attacks in 802.11 networks, *In Proc. Of WCNC*, IEEE Communications Society, 2004.

Fiehe, S., Riihijärvi, J., and Mähönen, P. 2010, Experimental study on performance of IEEE 802.11n and impact of interferers on the 2.4 GHz ISM band. In: Proceedings of the 6th International Wireless Communications and Mobile Computing Conference, 2010, pp 47–51.

He, C. and J. C. Mitchell, 2004. Analysis of the 802.11i 4-Way Handshake. *In Proceedings of the Third ACM International Workshop on Wireless Security (WiSe'04)*, Philadelphia, PA, October, 2004.

He, C. and J. C. Mitchell, 2005. Security Analysis and Improvements for IEEE 802.11i, *In Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS'05)*, pp. 90-110, 2005.

IEEE 802.11n 2004. http://en.wikipedia.org/wiki/IEEE_802.11i-2004

Jain, S. K. and K. Garg, 2009. A hybrid model of defense techniques against base station jamming attack in wireless sensor networks, in *Proceedings of the 2009 First International Conference on Computational Intelligence, Communication Systems and Networks*, 2009, pp. 102–107.

Jarupan, B., and Ekici, E. 2011 A survey of cross-layer design for VANETs. Ad Hoc Networks 9(5):966–983.

Jerbi, M., Marlier, P., and Senouci, S. 2007. Experimental assessment of V2V and I2V communications. In: IEEE Internatonal Conference on Mobile Ad Hoc and Sensor Systems, 2007, pp 1–6.

Lazos, L. , S. Liu, and M. Krunz, 2009. Mitigating control-channel jamming attacks in multi-channel ad hoc networks, in *Proceedings of the 2nd ACM Conference on Wireless Network Security*, 2009, pp. 169–180.

Mahajan, R., Zahorjan, J., and Zill, B. 2007. Understanding wifi-based connectivity from moving vehicles. In: Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement, 2007, pp 321–326.

Mahonen, P., J. Rihijarvi, and M. Petrova, 2004. Automatic Channel Allocation for Small Wireless Local Area Networks using Graph Coloring Algorithm Approach, in *Proc. IEEE Int. Symposium on Personal Indoor and Mobile Radio Communications*, pp. 536-539, Sept. 2004.

Medvedev, I., Bjerke, B., Walton, R., Ketchum, J., Wallace, M., and Howard, S. 2006. A comparison of MIMO receiver structures for 802.11n WLAN - performance and complexity. In: IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications, 2006, pp 1–5.

Mishra, A., V. Brik, S.Banerjee, A. Sreenivasan, and W. Arbaugh, 2006. A Client-driven Approach for Channel Management in Wireless LANs, in *Proc. 25th IEEE International Conference on Computer Communications (INFOCOMM'06)* 2006.

Misra, S., R. Singh, and S. V. R. Mohan, 2010. Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system, *Sensors*, vol. 10, pp. 3444–3479, 2010.

Mpitziopoulos, A., D. Gavalas, G. Pantziou, and C. Konstantopoulos, 2007. Defending wireless sensor networks from jamming attacks, in *IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, Sept. 2007, pp. 1 –5.

Muraleedharan, R. and L. A. Osadciw, 2006. Jamming attack detection and countermeasures in wireless sensor network using ant system, in *SPIE the International Society for Optical Engineering*, 2006.

Pape, D., Arant, M., Brock, W., Delorenzis, D., LaClair, T., Lim, A., Petrolino, J. and Spezia, A. 2011. U31: Vehicle Stability and Dynamics: Electronic Stability Control, Final Report to National Transportation Research Center, Inc., U.S. Department of Transportation, Research and Innovative Technology Administration, Grant #DTRT-06-G-0043.

Paul, T., and Ogunfunmi, T. 2008. Wireless LAN comes of age: Understanding the IEEE 802.11n amendment. IEEE Circuits and Systems Magazine 8(1): 28–54.

Paul, T., and Ogunfunmi, T. 2009. Evolution, insights and challenges of the PHY layer for the emerging IEEE 802.11n amendment. IEEE Communications Surveys Tutorials 11(4):131–150.

Paul, U., Crepaldi, R., Lee, J., Lee, S.J., and Etkin, R. 2011. Characterizing WiFi link performance in open outdoor networks. In: IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, 2011, To appear.

Pelechrinis, K., M. Iliofotou, and S. Krishnamurthy, 2011. Denial of service attacks in wireless networks: The case of jammers, *IEEE Communications Surveys Tutorials*, vol. 13, no. 2, pp. 245 –257, quarter 2011.

Stallings, W. 2004. IEEE 802.11: Wireless LANs from a to n. IT Professional 6(5):32–37.

Tague, P., D. Slater, R. Poovendran, and G. Noubir, 2008. Linear programming models for jamming attacks on network traffic flows, *6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops*, pp. 207–216, April 2008.

Wang, J., and Hsieh, M.F. 2009. Vehicle yaw-inertia- and mass-independent adaptive steering control. Proceedings of the Institution of Mechanical Engineers, Part D (Journal of Automobile Engineering) 223: 1101-1108.

Wang, L. and Srinivasan, B., 2010. "Analysis and Improvement over DoS Attacks against IEEE 802.11i Standard," *In Proc. Of Second International Conference on Network Security* (IEEE) 2010.

Wood, A., J. Stankovic, and S. Son, 2003. JAM: a jammed-area mapping service for sensor networks, in *24th IEEE Real-Time Systems Symposium*, Dec. 2003, pp. 286–297.

Xiao, Y. 2005. IEEE 802.11n: Enhancements for higher throughput in wireless LANs. IEEE Wireless Communications 12(6):82–91.

Xing, X., E. Shakshuki, D. Benoit and T. Sheltami, 2010. Security Analysis and Authentication Improvement for IEEE 802.11i Specification, *In Proceedings of IEEE "GLOBECOM"*, 2008.

Xu, W., W. Trappe, Y. Zhang, and T. Wood, 2005. The feasibility of launching and detecting jamming attacks in wireless networks, in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2005, pp. 46–57.

Xu, W., K. Ma, W. Trappe, and Y. Zhang, 2006. Jamming sensor networks: attack and defense strategies, *IEEE Network*, vol. 20, no. 3, pp. 41–47, may-june 2006.

Yang, Z., B. Gu, A. Champion, X. Bai and D. Xuan, 2009. "Link Layer Protection in 802.11i WLANs with Dummy Authentication," *In Proc. of ACM Conference on Wireless Network Security (WiSec)*, March 2009 (short paper).