2018

On The Security And Quality Of Wireless Communications In Outdoor Mobile Environment

Sharaf J. Malebary
University of South Carolina

Recommended Citation

Malebary, S. J.(2018). *On The Security And Quality Of Wireless Communications In Outdoor Mobile Environment.* (Doctoral dissertation). Retrieved from https://scholarcommons.sc.edu/etd/4808

ON THE SECURITY AND QUALITY OF WIRELESS COMMUNICATIONS IN OUTDOOR MOBILE ENVIRONMENT

by

Sharaf J. Malebary

Bachelor of Science
King Abdul-Aziz University, 2005

Master of Engineering
University of South Carolina, 2008

Submitted in Partial Fulfillment of the Requirements

For the Degree of Doctor of Philosophy in

Computer Science and Engineering

College of Engineering and Computing

University of South Carolina

2018

Accepted by:

Wenyuan Xu, Major Professor

Manton Mathews, Chair, Examining Committee

Csilla Farkas, Committee Member

Chin-Tser Huang, Committee Member

Marco Valtorta, Committee Member

Adel Abdullah, Committee Member

Cheryl L. Addy, Vice Provost and Dean of the Graduate School

ABSTRACT

The rapid advancement in wireless technology along with their low cost and ease of deployment have been attracting researchers academically and commercially. Researchers from private and public sectors are investing into enhancing the reliability, robustness, and security of radio frequency (RF) communications to accommodate the demand and enhance lifestyle. RF base communications -by nature- are slower and more exposed to attacks than a wired base (LAN). Deploying such networks in various cutting-edge mobile platforms (e.g. VANET, IoT, Autonomous robots) adds new challenges that impact the quality directly. Moreover, adopting such networks in public outdoor areas make them vulnerable to various attacks (regardless of the attacker motive). Therefore, the quality and security of the communications cannot be neglected especially when developing outdoor wireless applications/networks.

While some wireless applications and platforms aim to provide comfort and infotainment, others are more critical to protect and save lives. Thus, the need for mobile broadband connections has been increased to accommodate such applications. The FCC took the first step to regulate and assure the quality when using these technologies by allocating spectrums and issuing standards and amendments (e.g. IEEE802.11a, b, g, n, and p) to deliver reliable and secure communications.

In this dissertation, we introduce several problems related to the security and quality of communications in outdoor environments. Although we focus on the ISM-RF bands

UHF and SHF (licensed and unlicensed) and their applications when solving quality and security issues nevertheless, the concept of propagating signals through the air for communications remain the same across other ISM bands. Therefore, problems and their solutions in this work can be applied to different wireless technologies with respect to environment and mobility.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AC	Access Categories
AC[BE]	Access Category [Best Effort]
AC[BK]	Access Category [Background]
AC[VI]	Access Category [Video]
AC[VO]	Access Category [Voice]
ACC	Adaptive Cruise Control
ACK	Acknowledgment
AIFS	Arbitrary Inter frame Spacing
BCON	Beacon
BPSK	Binary Phase Shift Keying
BS	Base Station
BSM	Basic Safety Message
BSS	Basic Service Set
CCH	Control Channel
CP	Cyclic Prefix
CRC	Cyclic Redundancy Code
CSI	Channel State Indication
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CV	Connected Vehicles
CW Max	Contention Window Maximum

CW Min	Contention Window Minimum
DCC	Distributed Congestion Control
DCF	Distributed Coordination Function
DIFS	DCF- Inter frame Spacing
DOT	Department of Transportation
DSRC	Dedicated Short Range Communication
EDCA	Enhanced Distributed Channel Access
EIFS	Extended Inter Frame Spacing
EIRP	Effective Isotropic Radiated Power
ERP	Extended Rate PHY
ESS	Extended Service Set
ETC	Electronic Toll Collection\Communication
FEC	Forward Error Correction
FFT	Fast Fourier Transform
HCCA	Hybrid Controlled Channel Access
HCF	Hybrid Coordination Function
ICI	Inter Carrier Interference
IEEE	Institute of Electrical and Electronics Engineers
IFFT	Inverse Fast Fourier Transform
IFS	Inter Frame Spacing
ISI	Inter Symbol Interference
ITS	Intelligent Transportation System
IVC	Inter Vehicle Communication
LOS	Line Of Sight
LTS	Long Training Symbol

MAC	Medium Access Control
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
MTU	Maximum Transmission Unit
NAV	Network Allocation Vector
OBU	On-Board Unit
OFDM	Orthogonal Frequency Division Multiplexing
ISO/OSI	International Standards Organization Open System Interconnection
PCF	Point Coordination Function
PDR	Packet Delivery Ratio
PDSR	Packet Delivery Send Ratio
PHY	Physical Layer
PLCP	Physical Layer Convergence Protocol
PLME	Physical Layer Management Entity
PMD	Physical Medium Dependent
PPDU	PLCP Protocol Data Unit
PSDU	PLCP Service Data Unit
PSR	Packet Send Ratio
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QoS-Data	Quality of Service Data packet
QPSK	Quadrature Phase Shift Keying
RBC	Random Back off Countdown
RSU	Road Side Unit
RTS/CTS	Request/Clear To Send

SCH	Service Channel
SIFS	Short Inter Frame Spacing
SINR	Signal to Interference to Noise Ratio
SNR	Signal to Noise Ratio
SS	Signal Strength
STA	Station
STS	Short Training Symbol
TCP	Transmission Control Protocol
UDP	User Diagram Protocol
UTC	Universal Time Coordination
VANET	Vehicular Ad-Hoc Network
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to Vehicle and Vehicle to Infrastructure
WAVE	Wireless Access in Vehicle Environment
WBSS	WAVE Basic Service Set
WME	WAVE Management Entity
WSA	WAVE Service Advertisement
WSMP	WAVE Short Message Protocol

CHAPTER 1

INTRODUCTION

Technologies have been evolving rapidly over the last decade. In particular, wireless (Radio Frequency-RF) communications have been gaining a wide interest from governments, researchers, and companies. The low cost along with ease of deployment and maintenance, have made wireless technology a fruitful research field academically and commercially.

Nowadays, different forms of wireless communications can be seen everywhere. Smart phones, computers, televisions, appliances, aerial vehicles and even cars have been manufactured and employed with wireless capabilities. When wireless technology was first discovered, it used to be a luxury not everyone can afford. Nowadays, their affordability, capability, and reliability have made the new era moves toward utilizing the technology to lower expenses and provide safety in almost every field (military, health, industry, education ...etc.)

In 2009, US-DOT released a statistical analysis showing that cars are the leading cause of death for people ages between 4 to 34 years old. Statistics showed that more than 33000 deaths and 5,800,000 crashes per year in addition to over $78 billion cost of urban congestion are caused by vehicles [20]. Although several studies have investigated threats on roads and tried to propose solutions based on the cause of accidents (human, environment, or vehicle –related), the US-DOT have acknowledged cars impact on economy and people’s safety which led the department to conclude that roads are no longer as safe to drive on as used to.

The new era is moving toward employing wireless communications to make cars intelligent to save resources (financially), enhance safety of drivers, and provide comfort. Therefore, car manufacturers and governments have been cooperating and investing into proposing new solutions. In the early 2000s, Vehicular Ad-hoc Network (VANET) was only seen as a one-to-one application of Mobile Ad-hoc Network (MANET). Since then, VANET have been developed into research field until officially introduced earlier in 2005. The unique property of VANET is the collaboration between vehicles and networks technologies. Therefore, VANET has attracted cars manufacturers, governments, researchers, and companies. As a result of these efforts, VANET was proposed and standardized by IEEE group over the globe. Consequently, cars’ manufacturers started investing to research and produce “wireless cars”. For instance, Volkswagen has enabled their cars to talk to each other [64], while Google have successfully made a fully automated car that can drive and park itself [65]. Moreover, Cadillac (General Motors’ Company) has promised to release its first vehicle equipped with ITS (Intelligent Transport System) using DSRC (Dedicated Short-Range Communication) in late-2015 [66].

While VANET has been gaining popularity, its security and privacy have been a concern. Since drivers’ safety is the ultimate goal behind proposing VANET, many security risks needed to be addressed to ensure the normal operation of the network and hence, enhance safety on roads. Typical issues such as the reliability and availability of the network in highly changeable mobile environment have been addressed however; they are yet to be finalized. Although VANET shows a potential enhancement of safety and comfort on roads, the new technology (based on inserting Wireless Access in Vehicle Environment WAVE) is still vulnerable to most of attacks that work against radio frequency communications. Yet, the great potential of the technology led to the development of many VANET-based applications and deployment by IT-companies, governments (e.g, toll-collections), and cars' manufacturers (e.g, traffic congestion and emergency vehicle warning systems).

Since drivers' safety is the main goal behind proposing VANET, and it is dependent on the successful delivery of early warning messages. Therefore, establishing and maintaining reliable communications links between nodes is crucial and challenging due to the nature of RF-communications (using wireless medium as communications mean). Moreover, the characteristics of the outdoor environment (encompass high mobility of nodes, irregular surrounding noise, and unpredictable weather phenomena), has made VANET a challenging research field.

Here we focus on the security aspect of VANET. We investigate the feasibility of launching intentional interference (jamming) attack to disrupt the normal operation of the network. We analyze the security risks caused by intentional interference attacks in outdoor mobile environments from message delivery aspect. We also provide a low-latency jamming detection solution to solve the intentional interference problem in outdoor mobile environment.

1.1 VANET Overview

Since VANET was proposed earlier in 2005, many terminologies and acronyms have been used that refer to the same technology concept (vehicular networking). Although these terms may differ in technical low-level details, but generally they are the same. The most commonly found terms are:

- ITS (Intelligent Transport Systems)
- IVC (Inter-Vehicle Communication)
- DSRC (Dedicated Short Range Communication)
- WAVE (Wireless Access in Vehicle Environment)

Throughout this dissertation we may use variety of these terms to refer to the same technology except when explicitly stated.

VANET consists of two types of wireless nodes. The combination of i) cars equipped with wireless capabilities, ii) and infrastructures towers like nodes forms a VANET. This allows communications among and between Infrastructures (Road-Side nodes) and cars (mobile nodes) Fig.1.1. By doing so, many VANET based applications were proposed and developed to serve the ultimate goal of VANET (enhancing safety and comfort on road). These applications can be categorized based on their serviceability into: i) Safety, ii) Traffic Management, and iii) Maintenance & Comfort enhancement -applications Table.1.1. While some of these applications are developed to provide comfort and infotainments, some others can save lives and money.

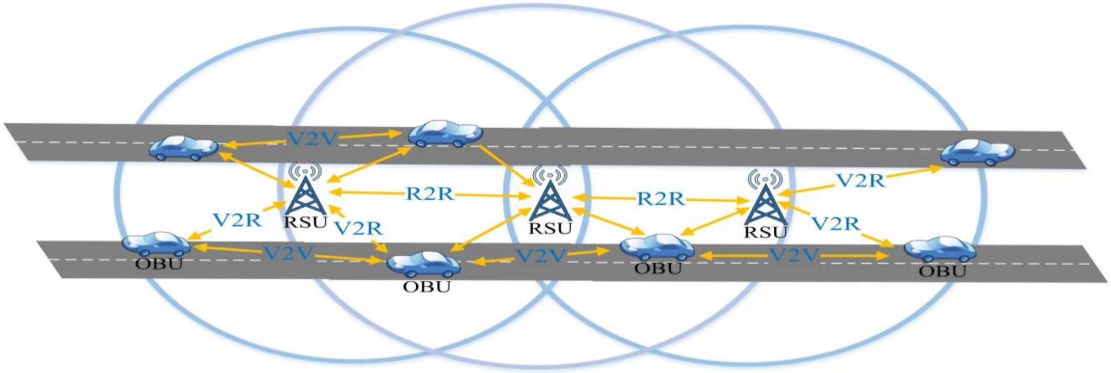


Figure 1.1: Nodes' and Communications' Types in VANET

Table 1.1: Examples of some VANET Based Applications

VANET Based Applications		
Safety	**Traffic Management**	**Maintenance and Comfort**
Traffic Signal Violation Warning	Highway Merge Assistance	Safety Recall Notice
Stop Sign Violation Warning	Cooperative Cruise Control	Just-in-time repair notification
Left-Turn Assistance	Cooperative Platooning	Wireless Diagnosis
Intersection Collision Warning	Fleet Management	Visibility Enhancer
Pedestrian Crossing Information	Adaptive Speed Limit Based on Road Conditions	Cooperative glare reduction/Headlamp aiming
Emergency Vehicles	HAZMAT Cargo Tracking	Parking Spot Locator
Vehicle Safety Inspection	Electronic Toll Payment	GPS Correction
Electronic License Plate		Instant Messaging Between Vehicles
Electronic Driver License		Mobile Access to Vehicle data
Stolen Vehicle Tracking		POI Notification
SOS Services		Fueling Info.
Pre-Crash Sensing		
Road Condition Warning		

1.2 STANDARDS AND SPECTRUM

VANET has been recognized globally, and different regions have allocated different spectrum, frequencies, and transmission ranges. Table.1.2 summarizes the global spectrum allocation dedicated for VANET uses in different regions.

Table 1.2: DSRC/WAVE GLOBAL SPECTRUM ALLOCATION

Region	Frequency (MHz)	Band	Range
North America (US)	5850 – 5925	75 MHz	1000 m
Japan	5770 - 5850	80 MHz	30 m
Europe	5795 - 5815	20 Mhz	15 – 20 m

In October 1999, the U.S. Federal Communication Commission (FCC) released an official announcement of allocating 75MHz spectrum in 5.9GHz range for Intelligent Transportation System (ITS) uses, which empowered by wireless communications Fig.1.2. The announcement dictates the FCC decision to use 5.850-5.925GHz band for a variety of

Dedicated Short-Range Communication (DSRC) uses to create more robust environment with higher noise resistance compared to the current 2.4GHz. [7]-[12]

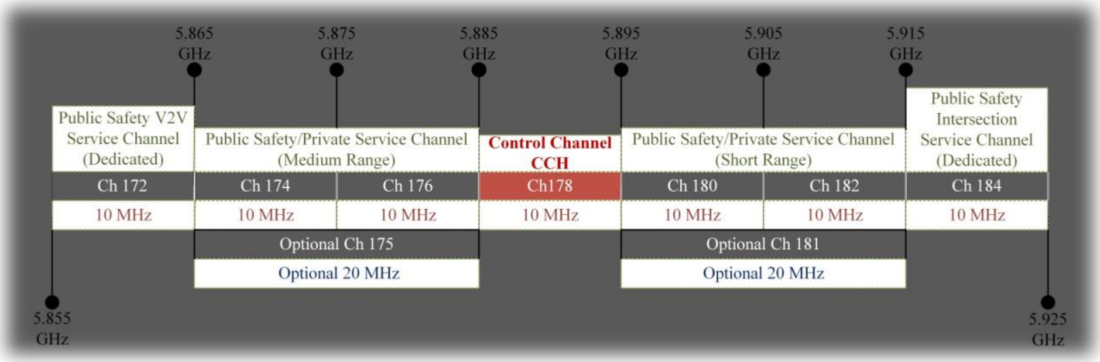
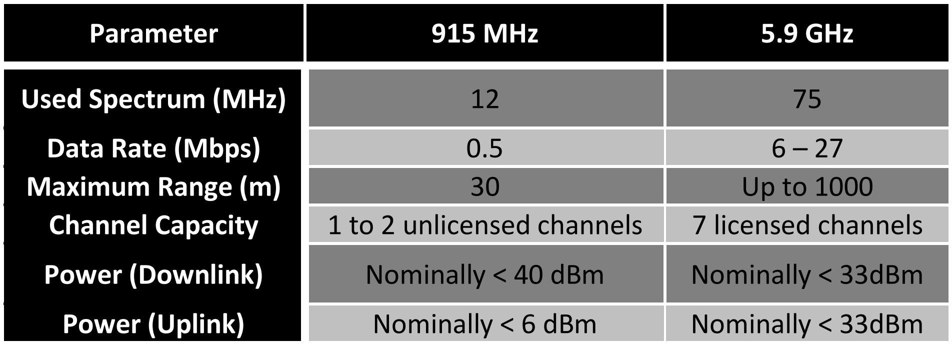


Figure.1.2: Spectrum Allocation for VANET Communications

DSRC/WAVE consists of a set of IEEE1609 standards for wireless access in vehicular environment. It is important to distinguish between the former DSRC standard in 915MHz range (used primarily in ETC applications), and the wireless access in Vehicular Environment (WAVE) standard approved for the current 5,9 GHz DSRC band Table.1.3.

Table.1.3: DSRC 915MHz Vs. 5.9 GHz Comparison



Parameter	915 MHz	5.9 GHz
Used Spectrum (MHz)	12	75
Data Rate (Mbps)	0.5	6 – 27
Maximum Range (m)	30	Up to 1000
Channel Capacity	1 to 2 unlicensed channels	7 licensed channels
Power (Downlink)	Nominally < 40 dBm	Nominally < 33dBm
Power (Uplink)	Nominally < 6 dBm	Nominally < 33dBm

The IEEE1609 family, IEEE802.11p, and Society of Automotive Engineers (SAE-J2735) standards illustrate the WAVE protocol stack Fig.1.3. They define the main architectural components of two types of nodes (On Board & Road Side –Units), WAVE interface, and describe the functionality of WAVE based applications (approved in 2010).

- IEEE P1609.0 “Draft Standard for Wireless Access in Vehicular Environments (WAVE) – Architecture.”
- IEEE 1609.1 “Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) – Resource Manager.”
- IEEE 1609.2 “Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) – Security Services for Applications and Management messages.”
- IEEE 1609.3 “Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services.”
- IEEE 1609.4 “Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-Channel Operations.”
- IEEE P1609.11 “Over-the-Air Data Exchange Protocol for Intelligent Transportation Systems (ITS).”
- IEEE 802.11p “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment: Wireless Access in Vehicular Environments.”

The IEEE802.11p standard is an amendment to IEEE802.11 (known as Wi-Fi) for WAVE applications. It adopts the OFDM PHY on 10MHz channels in 5.9GHz frequency band. The subcarrier spacing and supported data rate are halved and its symbol and guard intervals are doubled. Table.1.4 summarizes other OFDM parameters comparison which makes DSRC more robust and provides low-latency (50ms) in noisy environment.

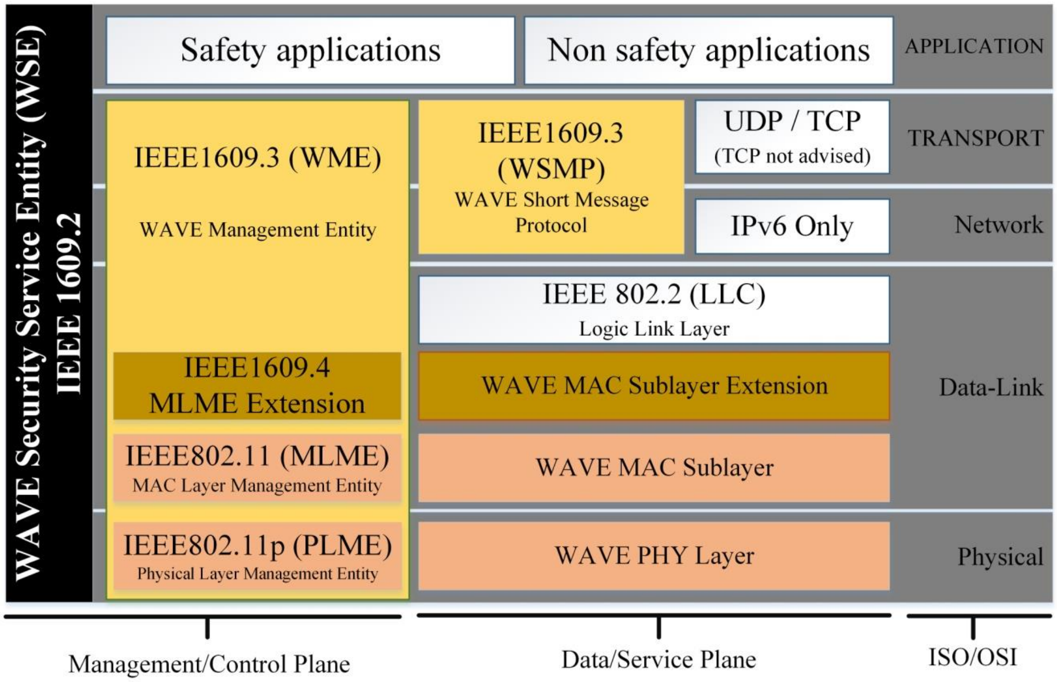


Figure.1.3: WAVE ISO/OSI Protocol Stack

Table.1.4: OFDM Wi-Fi Vs. OFDM WAVE Comparison

Parameter	WAVE	Wi-Fi
Spectrum (GHz)	5.9	2.4 and 5
Bandwidth (MHz)	10	20
Data Rate (Mbps)	3,4.5, 6, 9, 12, 18, 24, 27	6, 9, 12, 18, 24, 36, 48, 54
Modulation	No change	BPSK, QPSK, 16QAM, 64QAM
Data Subcarriers	No change	48
Pilot Subcarriers	No change	4
FFT/IFFT period (µs)	6.4	3.2
Subcarrier Spacing	0.15625	0.3125
Guard Interval (µs)	1.6	0.8
OFDM Symbol Interval (µs)	8	4
Preamble Duration (µs)	32	16

1.3 Channels Allocation, and Access modes

The FCC has allocated 75MHz of the spectrum in the 5.9GHz band for DSRC uses. The DSRC spectrum used in the IEEE802.11p standard is divided into seven 10MHz channels with data rates available from 3-27Mbps. One Control Channel (CCH-178) is designated for data management and transmitting important safety messages, and six other Service Channels (SCH-172, 174, 176, 180, 182, 184) used for exchanging non-safety data. Also offered is the option to combine two 10MHz Channels (174, 176) and (180, 182) to form a 20MHz channels (175 and 181) respectively with data rates from 6-54 Mbps.

Based on the standard regulations, there are four channel access options can be used in the CCH and SCH interval Fig.1.5. 1) Continuous: where vehicle stays in the CCH to exchange safety messages when available. 2) Alternating: by accessing the CCH to transmit safety messages and switches to SCHs to transmit non-safety messages at the beginning of each channel's interval. 3) Immediate: this option is specified to allow vehicles to have an immediate access to SCHs, after receiving an immediate request access, without waiting for the next SCH interval. 4) Extended: allows vehicles to remain in SCH without any pause for CCH access. Vehicles shall choose between continuous control channel or alternating service channel accesses Fig.1.4 depending on which is applicable, unless an immediate or extended access request received.

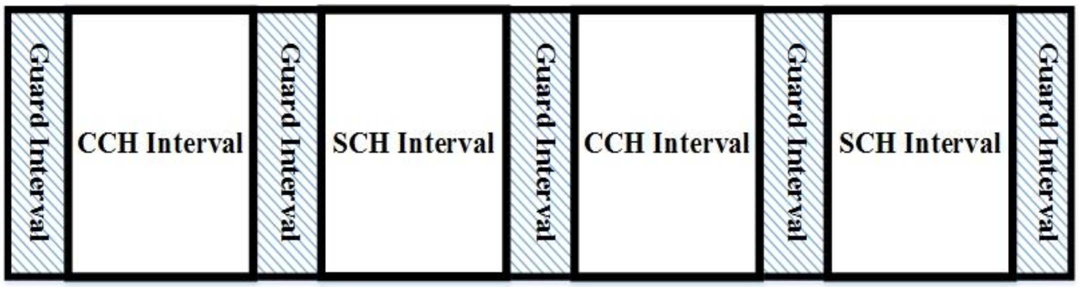


Figure 1.4: Alternating Channel Access Option in 802.11p Networks

1.4 DSRC/WAVE Devices

There are two classes of devices in a WAVE system: Vehicles equipped with On-

-Board Units (OBUs) and infrastructures towers-like Road-Side Units (RSUs). OBU and RSU are equivalent to Mobile Station (MS) and Base Station (BS) in the cellular network. As a result, the combination of RSUs and OBUs enables mainly two classes of communications, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Fig.1.6.

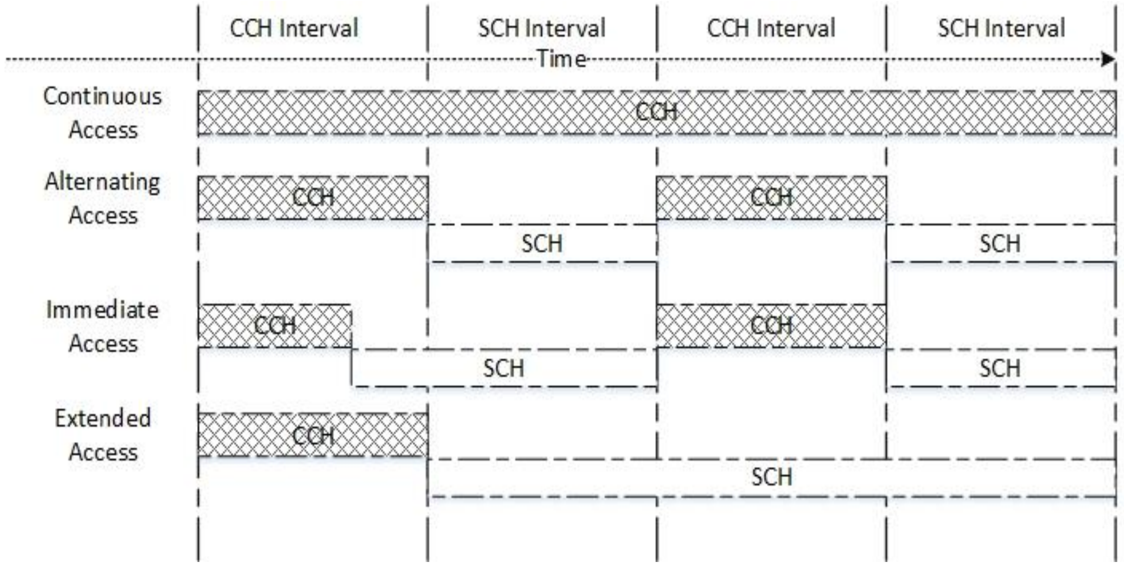


Figure.1.5: Receiver Multi-Channel Access Operations defined by IEEE1609 standards for the MAC Sub-layer extension in DSRC protocol stack (CCH, SCH: Control, Service channel)

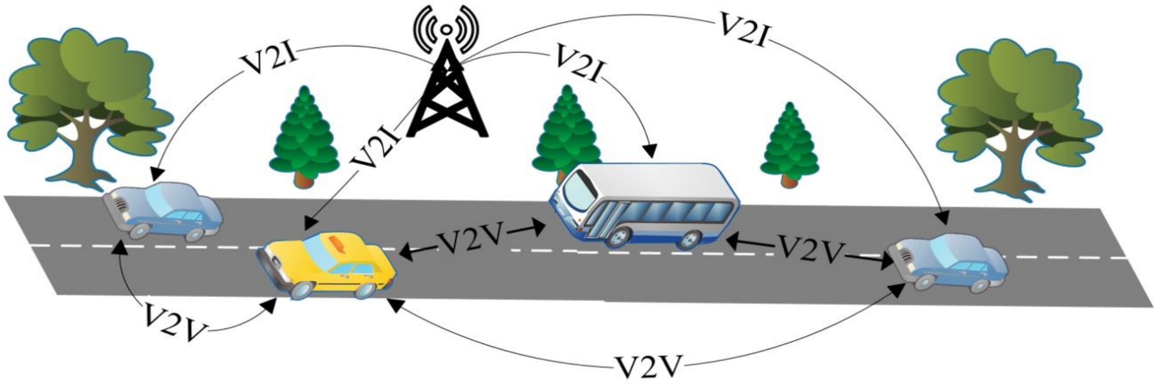


Figure.1.6: Two Communication's classes among wireless nodes in VANET

Although other terms may be seen such as Vehicle-to-roadside-unit (V2R) and Vehicle-to-OBU/RSU (V2X), they are still derived from the main communications V2V and V2I.

- RSUs are stationary towers-like infrastructures deployed on the side of roads. RSUs are expected to provide coverage (up to 1000m) to disseminate, exchange, and forward data among nodes. Although RSUs are expected to serve as the main component to spread safety messages within their range, yet no clear definition exists regarding their placements on the roads.
- OBUs are vehicles equipped with wireless capabilities to exchange data on roads. These data can be safety related or application-based service data.

Based on the different mobility nature of RSUs and OBUs, several challenges appeared very quickly concerning communications range, noise, multipath, and Doppler Effect which will be discussed in the next chapter [2], [11], [15], [19].

1.5 SUMMARY

The new era targets at making cars more intelligent to enhance drivers’ safety and comfort. Equipping cars with wireless communication capabilities was the first step toward achieving such a goal. The Intelligent transportation system (ITS), which is a national program [7], intended to use modern computers and communications to make driving safer, smarter, faster and more convenient. To achieve these goals, ITS provides automatic toll collection, traveler information system, intelligent commercial vehicles and intelligent traffic control systems. The main goal of ITS program is to enhance safety and comfort on roads by exchanging information among cars.

CHAPTER 2

CHALLENGES

VANET is expected to enhance safety so it must be extremely robust and able to cope with various unpredictable environmental conditions (high mobility of nodes, changing weather, irregular noise, and obstacles). Various conditions pose different impact on the performance of the wireless communications (the delivery of safety messages). Failing to receive safety messages may cause accidents, traffic jam, or violations which cost lives and money. For those reasons many researchers started addressing and analyzing the impact of different conditions and their effect on the wireless communications. VANET is expected to operate outdoor in mobile environment, where roads' and environmental conditions are constantly changing. Moreover, VANET encompasses highly changeable mobility (speed and direction). Here we summarize the main natural (unintentional) factors that make VANET uniquely challenging.

2.1 MOBILITY AND COMMUNICATION

Vehicles speed, direction, and density are constantly changing (matter of seconds). Vehicles by nature are expected to be mobile at random speed and direction. For instance, a vehicle may experience a sudden and hard braking due to a construction zone or an accident in a highway road. This introduces a great challenge especially when dealing with delivery and latency of safety messages. Hence, regulations recommend and favor generating UDP network traffic in VANET (including safety messages). Unlike TCP (delivery can be verified by Acknowledgment -ACK), ACKs are not applicable in UDP traffic. In order to enhance safety on roads, the delivery of safety messages must be ensured when transmitted. The utilization of UDP to generate safety related messages along with the mobility freedom of vehicles nodes (can leave communication range anytime) have made VANET a challenging area for researchers and VANET-app developers.

2.2 Road Conditions

VANET is expected to operate in outdoor environment where vehicles' mobility and the variation in transmission environment (urban, desert, forest and highway) have a great impact in the quality of the wireless communications. The quality (power) of wireless signals is easily influenced by obstacles in the space (e.g. trees and buildings), weather conditions (e.g. snow and rain), and mobility (e.g. speed and direction). Hence, the quality of communications need to be verified under irregular extreme various conditions such as vehicles density, surrounding obstacles, geographical characteristics and weather changes, to evaluate the impact of these conditions on the connectivity and delivery of messages delivery. It is infeasible and challenging to test all conditions since one can't change weather to evaluate the network performance when it is snowing or lightening for example. Moreover, it is very costly and dangerous to try to replicate real scenarios (e.g. congested road), which makes it very challenging to conduct experiments and evaluate results.

2.3 Environment (Noise)

Wireless communications –in general- can be easily interfered with, depending on the environment operating in (outdoor/indoor). Although VANET uses DSRC in 5.9GHz spectrum to provide higher noise resilience in outdoor environments, interference can still happen due to the increase in number of vehicles (engine and communication noise), weather changes, impact of other wireless devices (cellular, Wi-Fi, …etc). In wireless communications, all undesired collected signals are referred to as white noise regardless the generating source. Noise degrades the signal quality and strength that carry information from the transmitter to the receiver. Communications can be disrupted and may be blocked completely in very noisy environment. The ratio between the desired signal power (P_{signal}) to the surrounding noise power (P_{noise}) is called Signal-to-Noise Ratio (SNR) represented as follow:

$$SNR = P_{signal} / P_{noise}$$

In outdoor environment, there are more various and random processes occur in natures that contribute to degrading the signal quality and the network performance. It is infeasible and challenging to address all variables that can cause interference, especially the ones caused by natural phenomena (heat, snow, rain, …etc.). Also, the impact on the signal quality is constantly changing based on the surroundings.

2.4 SUMMARY

VANET uses wireless medium as communications means. Thus, it inherits same security risks and vulnerabilities of other types of wireless networks. Moreover, deploying and operating VANET outdoor adds on extra challenges due to natural characteristics of the environment i.e., highly changeable mobility of nodes, surrounding noise, and road conditions. Also, various technical factors, including modulations, encoding, frame size, data rate CP and unused subcarriers, have a great impact on the communications' performance. The aforementioned challenges have made VANET a hot and challenging research field especially in terms of security and quality of service. To achieve the ultimate goal behind proposing VANET (saving lives), the technology must be extremely robust and secured to cope with the rapid changes in the environment.

CHAPTER 3

INTENTIONAL INTERFERENCE ATTACKS

In the previous chapter, we discussed some of the challenges that undermines VANET’s ultimate goal of saving lives. We discussed various challenges which impact the wireless communications (V2V and V2I). The aforementioned challenges are due natural reasons (weather, obstacles, traffic jam, accidents, etc.), cause unintentional interference, and their impact can be mitigated. Several researches [21]-[23] have discussed the various unintentional environmental-phenomena and their effect on performance of the communications. Additionally, interfering with wireless communications can be considered not only a challenge but rather a threat when caused intentionally. Radio frequency interference attacks in VANET are not addressable through conventional security mechanisms. The high and freedom mobility along with operating outdoor makes detecting intentional interference a hard research problem. Simply, an attacker can disregard the protocols defining the medium access and continuously transmit RF signals to disrupt, block, or interfere with the normal operation of the wireless communications. This kind of attacks is referred to as jamming attacks. Many jamming attacks models were proposed as well as algorithms that solves the jamming problem in different wireless networks. However, applying same the methods to solve intentional jamming in vehicular networks is not feasible due the characteristics of the environment and communicating nodes. In this chapter, we give details about the jamming attacks’ operations, behaviors and their effect on the communication when targeting outdoor-VANETs.

3.1 OVERVIEW & RELATED WORK

Jamming style attacks target at interfering and disrupting the wireless communications among legitimate nodes that use wireless channels as communications medium. Jamming problems have been thoroughly studied by many researchers, military, companies, and governments. A common knowledge is that a jammer constantly emits RF signals to fill a wireless channel and block communications among legitimate nodes. Xu et al. [13] studied the feasibility of launching and detecting jamming attacks in wireless networks. They introduced different schemes and behaviors that jammers may adopt to launch powerful and more destructive attacks. They modeled several jamming techniques in different scenarios using MICA-z wireless motes, and showed how deceptive, random, and reactive jamming behaviors can greatly impact the performance of the wireless communications and still remain undetectable when applying conventional algorithms to detect constant jammers. They also proposed jamming detection and localization algorithms based on the consistency between the PDR (Packet Delivery Ratio- which defines the network performance) and the observed Signal Strength (SS) measured by legitimate wireless nodes. Although their work has been recognized and served as a benchmark for most of RF- jamming style attacks' research, applying the same strategy in VANET won't solve the jamming problem due to high mobility and irregular environmental changes. Moreover, jamming effect is not tolerable in VANET since jamming attacks block the disseminations and delivery of safety messages. Failure to receive early warning messages may cause accidents and deaths.

3.2 Jamming Models and Characteristics in VANET

VANET is supposed to make roads safer by ensuring proper dissemination and delivery of early warning and safety messages among vehicles in outdoor environments. Detecting jamming attacks in this kind of environments is challenging task. The attackers' freedom of mobility (stationary or roaming) and operation (jamming or sleep) in unpredictable environment contribute to jammers' goal (remain hidden when launching attacks). Detecting jammers becomes even more complicated and challenging depending on the adopted jamming behavior when launching the attacks. In this section, we discuss the different jammers mobility and behaviors that may be adopted when launching jamming attacks in vehicular network environment.

3.2.1 Jamming Mobility

Considering that VANET consists of both stationary (RSUs) and mobile (OBUs) nodes, a jammer may target at an RSU, an OBU, or randomly roam around. To model these jamming patterns, we consider the following mobility patterns of a jammer. We focus on highway roads, and we assume that jammers are interested in remaining undetected.

- Stationary: A not moving jammer is considered stationary. Such a jammer can be sitting in a parked car or at road side while launching attacks targeting stationary RSU or OBU vehicles. Jammers of this type can only distress the communications effectively where located depending on jamming range. Although jammers of this type have full control over choosing the attack location, remaining stationary for an extended period of time increases the chances of getting detected. Also, it is infeasible to expect attacker to remain stationary in a highway road due to raising suspicions.

- Targeting mobility: This type of mobile jamming intends to target a specific mobile node (vehicle). Targeting-mobile jammers stay in close range to one car to ensure the jamming effect throughout the attack period. Depending on the adopted jamming model, this type of mobility makes detecting jamming hard especially when combined with reactive jamming behavior (introduced in next subsection).
- Random mobility. Additionally, jammers may launch attacks while driving in their cars or motorcycles that keep them mobile without targeting at a chosen target. They can exhibit random and high mobility with no constrains depending on their mobility means (cars, motorcycles, drones …etc.)

3.2.2 Jamming Behavior

In addition to jammers' mobility, attacker may choose different jamming behaviors when launching attacks. Some of these jamming behaviors are more sophisticated than others based on the probability of remaining undetected.

- Constant: A constant jammer sends out random radio signals all the time without following any MAC protocols. The objective of this type of behavior is to prevent legitimate nodes from accessing communication channels, or corrupt nearby packets by emitting high power signals (interference) causing higher bit-error-rate (BER) at the receiver and consequently high packet drop rate. The constant jammer has full control over when to turn jamming signals on or off.
- Random: Launching jamming attack that blocks and interferes with communication consumes a large amount of energy. To reduce energy consumption, a jammer can alternate between sleep mode for t_S and jam for t_J seconds. Adopting this technique

allows jammers to have more control over energy consumption by altering (t_S & t_J) as needed. Random jamming operation and effect is similar to constant ones, except that the former has more control over the consumed power by alternating between jamming and sleeping modes.

- Reactive: Instead of targeting packets at the sender and prevent their transmission without considering channel’s conditions, sophisticated active jammers target at the receiver’s side. They constantly listen to the targeted channel, and once a jammer senses packets being transmitted, attacker immediately launches jamming attack and block packets from being received correctly. This particular jamming behavior is challenging to detect due the hidden nature of jamming (jamming signals overlap with the packet transmission).

The combination of the aforementioned behaviors and mobility can produce nine types of jammers. Instead of examining all nine, we focus on reactive jammers with all three types of mobility patterns. We reason focusing on reactive jamming behavior to their hidden nature which makes it hard to detect when present. Also, we believe that any method that can detect reactive jammers can identify constant and random jammers. Already in [1], authors have studied random and constant jammers in VANET and proposed detection algorithm, their method rely on the successful reception of at least one beacon, and are not effective against reactive jammers (indistinguishable from congestion scenarios). Thus, without loss of generality, we study and validate stationary reactive jammers, targeting mobility jammers, and random mobility jammers.

3.3 Jamming Effectiveness

When launching a jamming attack, an adversary doesn’t follow any medium access control protocols. Jammers can disrupt and completely block nearby communications. Depending on the jammer’s position when launching the attack, the whole network in that area is affected. Therefore, jamming impact need to be investigated further, especially its impact on the operation of an outdoor and highly mobile environment. Xu et al. studied the feasibility of launching and detecting jamming attacks in wireless networks [13]. They evaluated jamming impact and effectiveness in their work using Berkeley motes. Although their algorithm showed promising results, it is infeasible to apply their technique in VANET due to unique characteristics of the network (encompass high mobility and volatile topology). Thus, we present the three metrics (PDR, PSR, SS) that are widely used to evaluate the performance of the network. These metrics are closely related to the network performance and are used to identify abnormalities that any wireless network may encounter.

- Packet Delivery Ratio (PDR). The ratio of successful delivered packets to destination compared to number of packets that have been sent out by sender. In vehicle network, the density of vehicles is highly changeable and dependent on road conditions and the time of day. For instance, during rush hours or holidays, roads experience more traffic (congestion) which corresponds to observing lower PDR. Also, if a jammer exists, packets will suffer from intentional interference causing a significant drop in the PDR. Consequently, distinguishing between low PDR caused by congestion or jamming attack is impossible by relying on PDR as a single metric.

- Packet Send Ratio (PSR). The ratio of packets that are successfully sent out by a legitimate source compared to the number of packets it intends to send out in the MAC layer. In congested roads, vehicles tend to travel at much lower speed which entitles longer communication period between nodes. Consequently, channel observes more RTS/CTS (Request/Clear -to send) requests leading to higher drop in PSR. Additionally, when jammer presents, the noise introduced by jammer may hold the channel status as busy, which leads to an increase in node's back-off timer and delay to receive CTS response. Regardless whether road is congested or jammed, more packets will be buffered and discarded upon the arrival of new packets or when they timed-out causing low observed PSR. Therefore, it is inadequate to rely on PSR alone to identify congested or jammed channel especially in the presence of reactive jammer who's targeting at packets after being sent out.
- Signal Strength (SS). Is a powerful tool measured at receiver that defines the signal quality of the radio frequency signals that carry data from source to destination. Since wireless nodes can sample SS during any period of time (depends on the employed protocol), many researchers have been utilizing SS to detect jamming attacks in different wireless networks. In VANET, vehicles have the freedom to enter and exit communications' range at random speed. As a result, observing high SS may correspond to high vehicles intensity (congestion), or jamming attack. Also, in case of jammers adopting reactive behavior (stay hidden until packets being transmitted), a lower SS maybe observed when measured during the transmission period. Therefore, one can't rely on SS as a standalone metric to distinguish between jamming and congestion scenarios.

To summarize, we introduced three different mobility patterns and three jamming techniques that jammer may adopt when launching attacks. We presented three network metrics that have been used to evaluate the performance of any wireless networks. We also discussed the deficiency to rely on these metrics (PDR, PSR, and SS) individually to detect and distinguish between jamming attack scenarios and congested road ones.

CHAPTER 4

DETECTING JAMMING ATTAKS IN 802.11p NETWORKS

The development of wireless Vehicle Ad-Hoc Network (VANET) aimed to enhance road's safety and provide comfortable driving environment. This goal can be achieved by ensuring proper dissemination and reception of early warning and infotainment messages. Intentional jamming attack targets at interfering with the normal operation of the network by disrupting wireless communications. Since VANET uses wireless medium as communication mean in outdoor environment (highly changeable road conditions, atmospheric phenomena, and nodes behaviors), estimating the network performance is a challenging task. Also, applying conventional methods to monitor, analyze and secure the network is infeasible. The combination of various road conditions and random mobility of nodes (traveling speed and directions) makes detecting jamming attacks a unique problem. Failure to detect jammers poses a threat to people lives and economy. Thus, in order to evaluate network performance accurately, and achieve a reliable detection of jammers, first we identify the impact of vehicles density on the performance of the network in term of signal strength and packet delivery. Then, we study jamming effectiveness when adopting different mobility patterns (stationary, random, or targeting) and behaviors (constant, random, and reactive). We focus on analyzing jamming impact when adopting reactive behavior, and different mobility patterns. Finally, we propose a two-phase algorithm to detect the presence of jammers in outdoor mobile environment. We evaluate our proposed algorithm in various highway scenarios using simulation. It is worth mentioning that our approach shows promising results to detect different types of jammers accurately in IEEE802.11p network.

4.1 Road Conditions Analysis

Road conditions are unpredictable by nature. Many factors impact the traffic on road including but not limited to (vehicles density, obstacles, weather conditions, construction zones, traffic lights, and speed limit). Most of these factors tend to be the same when analyzing a specific road for a period of time (hours). The density of vehicles on a road stands to be the only variable that inclusive rapid change over short period of time (matter of seconds or minutes). For instance, road could pack up with cars simply because it is rush-hour, work zone or due to accidents. Regardless the cause, the increase in number of vehicles in a certain road suggests more communication within that area. Hence, network experiences higher throughput in that area. Once reaching certain threshold (close to reach the maximum network bandwidth), all communications will be dropped due to network congestion. As a result, lower PDR and higher Packet lost rate (PLR) are observed.

Conducting a real-world experiment is very costly, dangerous, and time consuming. Therefore, we consider using NCTUns 6.0 to evaluate the impact of vehicles' density on the performance of the network. It is reasonable to assume that using NCTUns as an evaluation tool is sufficient based on a comparison study [24]-[25]. We also studied the development of NCTUns 6.0 and how various variables are modeled based on the approved 802.11p standards to verify the accuracy of our results Appendix A. So, in order to evaluate the performance of the network, we constructed a highway road that consists of two lanes (common in US), and placed RSU at the edge of the road (to ensure maximum link-time between nodes). Each simulation case ran for period of time (the time needed by a car to enter the RSU range until exiting). We define nodes maximum transmission power of (28.8dBM) and broadcasting dissemination rate at 10 Basic Safety Messages per second (BSM/s). Each BSM was generated as UDP traffic and size of (200-500 bytes) according to 802.11p standards [12].

We start running first case with 1 vehicle which corresponds to vehicle traveling on idle interstate (commonly not busy) or at off-peak traffic time (e.g. after mid-night). It is worth mentioning that vehicle nodes were defined with collision avoidance behavior rules where they can freely accelerate, decelerate, and switch lanes based on road conditions. We incremented the number of vehicles (to simulate road traffic under different conditions) and observed the impact of various vehicles density on traveling speed, communication time, and network performance (in term of PDR, PSR, and SS). Results in Fig.4.1.A shows that when vehicle density reaches %52 -around 60 cars/lane- of the roads capacity [calculated by dividing road length per lane within RSU range (1000m) over the length of average size vehicle (6m)], a noticeable drop in PDR, and PSR occur due to slower traveling speed causing longer communications time and more data exchange among nodes. We also noticed a slight increase in the measured SS that can be justified as more noise (communication, thermal, etc.) generated due to high vehicle density. Additionally, when the drop in the PDR reaches more than %45, the measured SS tend to remain almost the same. The key observation is the relation between vehicles density, velocity, and flow intensity. Thus, we classify road conditions based on the nodes' density as follow:

- Normal Period. Represents low density of vehicles traveling at, or close to, the posted speed limit on that road. During this period, vehicles experience reliable communication links within RSU range until exiting. This period tends to be insignificance to the attacker interest due to the low number of cars.

- Rush-Hour Period. Vehicles are forced to travel at much lower speed when vehicle density exceeds a certain threshold. Nodes tend to observe much lower PDR and PSR which correspond to higher lost packet rate than in normal period Fig.4.1. Therefore, ensuring reliable delivery of safety messages is essential during this period. Failure to receive sensitive data may result drivers to fail to slow, reroute, or stop in timely manner to avoid crashes.
- Incident Period. When number of vehicles is high and close to the capacity of the road, vehicles experience what's called a traffic jam (hours of non-moving or stop-and-go traffic). This tends to be the most favorable and effective period for jammers to launch their attack and remain undetected. The significance of this period is the tight relation between vehicles density and the probability of incidents to occur (high density corresponds to high probability of accident to occur).

4.2 Detection Algorithm

In this section, we propose a two-phase algorithm: (i) Initialization and (ii) Detection, to detect jammers based on the consistency between SS and Packet Delivery/Send Ratio (PDSR). Since road conditions vary from road to another, we consider vehicles density on road to serve as dynamic variable that correspond to the various conditions on roads.

- **Initialization Phase –Ip**. This phase may be conducted during a guaranteed time of non-interfered network operation (easily achieved by monitoring SS distribution over initialization time period (T_{ipt}), or equipping RSU with SS meter to filter out any amplified or unwanted measurements). Also, Initialization Phase (Ip) must be conducted when vehicles' density is relatively high, i.e. rush-hour, which easy to find depending on the road that RSU being deployed at. During this phase, RSU will calculate and collect (PDSR, SS, PLR) Packet-delivery/send-ratio, signal strength and packet lost rate in a table for T_{ipt}. Once the initialization period timer T_{ipt} expires, RSU will find upper bound (SS) value that would have produced a particular PDSR in non-jammed-rush-hour scenario [$PDSR_j$, Max(SS_j)]. After forming the table, RSU will assign two threshold values γ_{PDSR} and γ_{PLR}, the maximum $PDSR_j$ and the minimum PLR_j respectively, calculated during (T_{ipt}). Then a simple regression will be conducted to build a relation between (PDSR, SS) values for all ($PDSR_x$) that have not been observed and are less than the set threshold (γ_{PDSR}). Finally, each RSU node will calculate and set periodic monitoring timer (T_{wind}) by calculating the needed time by a car to enter and exit that RSU range denoted [T_{Cap}= road length within RSU range(L_{oR}) over the posted speed limit on road(SL_{oR})]. Upon the completion of this phase, each RSU will have a table contains an upper bound SS value to produce a particular PDSR, a periodic monitor window (T_{wind}), and two thresholds (γ_{PDSR}, γ_{PLR}) Table 4.1. It is worth mentioning, the collected data including thresholds will vary from one RSU to another depending on the roads that been deployed on.

- **Detection Phase with consistency check.** RSU will monitor (PDSR, SS) and calculate PLR every time window (W_{PLR}). When the observed PDSR and PLR exceed γ_{PDSR} and γ_{PLR} set during Ip, a consistency check is performed C_Check(Max(PDSR), SS) to check whether the low observed PDSR is consistent with the measured SS. The C_Check function, Table 4.3, takes an input

(Max(PDSR), SS) as pair and check whether the measured SS is consistent with the observed PDSR by checking the ($PDSR_{Ip}$, SS_{Ip}) table generated during the initialization period. The Boolean C_Check return decides whether the low observed PDSR is due jamming attack, or a typical congested road. The detector will also return “normal state” when T_{wind} runs out with no abnormalities Table 4.2.

Table.4.1: Jamming Detection Algorithm [Initialization Phase]

```
Algorithm 1: [Initialization phase]
Input: $T_{ip,} L_{oR}, SL_{oR}$
Output: $(PDSR_j, SS_j), (PDSR_x, SS_x), \gamma_{PDSR}, \gamma_{PLR}, T_{wind}, W_{PLR}$
for (j=1, j<= $T_{ip}$, j++) do
    Sum = 0
    for (i = j-1 → i=j) do
        Data[i] = ($PDR_i, PSR_i, SS_i, PLR_i$)
        Sum = Sum++
    end
    $PDSR_j = (\sum PDR_i + \sum PSR_i) / 2Sum$
    $SS_j = \{SS_i, SS_{i+1}, SS_{i+2}, \ldots\}$
    $PLR_j$ = Average ($PLR_i$)
    Data[j] = ($PDSR_j, SS_j, PLR_j$)
end
$T_{Cap} = L_{oR}/ SL_{oR}, W_{PLR}, T(PLR_j), T_{wind} = T_{Cap}/W_{PLR}$
$\gamma_{PDSR} = Max(PDSR_j \mid PDSR_j \in$ Data[j])
$\gamma_{PLR} = Min(PLR_j \mid PLR_j \in$ Data[j])
foreach $PDSR_j \in$ Data[j]
    Find upper bound $MAX(SS_i) \in SS_j$ that would produce $(PDSR_j)$
end
foreach $PDSR_x \notin$Data[j], and $PDSR_x < \gamma_{PDSR}$ do
    Conduct simple regression to build a relation between ($PDSR_x, SS_x$)
    Data[x] = ($PDSR_x, SS_x$)
end
return ($\gamma_{PDSR}, \gamma_{PLR}, T_{wind}, W_{PLR}$, Data[j], Data[x])
```

Table.4.2: Jamming Detection Algorithm [Detection Phase]

```
Algorithm 2: [Detection phase]
Input: $\gamma_{PDSR}$, $\gamma_{PLR}$, $T_{wind}$, $W_{PLR}$
Output: State
Initialize: Counter = 0, State = NORMAL
While (Counter < Size[$T_{wind}$]) do
    Counter++
    for each $W_{PLR}$ do
        Calculate ( $PDSR_J$, $SS_j$, $PLR_j$)
        if ($PLR_j$ > $\gamma_{PLR}$) && ($PDSR_j$ < $\gamma_{PDSR}$) then
            if C_Check($MaxPDSR_j$, $SS_j$) == True then
                Counter = 0
                State = (CONGESTED)
            else
                Counter = 0
                State = (JAMMED)
            end
        end
        return (State)
        State = (NORMAL)
    end
end
return (State)
```

4.3 Experiments and Evaluations

In order to evaluate our algorithm, we simulate a two-lane highway road of 1000 meter length (maximum RSU range) with different vehicle density (1-100 OBUs). We define same parameters mentioned in section4.1. [refer to Appendix B for details] We considered free space and shadowing propagation model which is more appropriate when simulating outdoor environment. Observations from simulators' results are summarized as follow.

- In Non-Attacker cases, we observed a significant drop in network performance when vehicles occupied more than %52 of the maximum road capacity. Thus, we assign this value (52%) as vehicle density threshold (approx. 60 cars) that corresponds to the road's conditions during rush hour (congested road) to run the Initialization phase -Ip. After running experiments and collecting data, we plotted our results shown in Fig.4.1.B with trend-line corresponding to threshold calculated during Ip.

Table.4.3: Jamming Detection Algorithm [Consistency Check]

```
Algorithm 3: Consistency_Check()
Input: $\gamma_{PDSR}$, $\gamma_{PLR}$, $T_{wind}$, $W_{PLR}$
Output: State
Initialize: Counter = 0, State = NORMAL
While (Counter < Size[$T_{wind}$]) do
|     Counter++
|     for each $W_{PLR}$ do
|     |     Calculate ( $PDSR_J$, $SS_j$, $PLR_j$)
|     |     if ($PLR_j$ > $\gamma_{PLR}$) && ($PDSR_j$ < $\gamma_{PDSR}$) then
|     |     |     if C_Check(MaxPDSR_j, SS_j) == True then
|     |     |     |  Counter = 0
|     |     |     |  State = (CONGESTED)
|     |     |     else
|     |     |     |  Counter = 0
|     |     |     |  State = (JAMMED)
|     |     |     end
|     |     end
|     |     return (State)
|     |     State = (NORMAL)
|     end
end
return (State)
```

- For Attacker scenarios, we implemented reactive jammer with multi-mobility capabilities (stationary, random, and targeting) and defined the mobility to follow the posted speed limit on road when possible (i.e. clear lane). Also, we defined fixed jamming power of 44dbm (such a device can be obtained for less than $200).

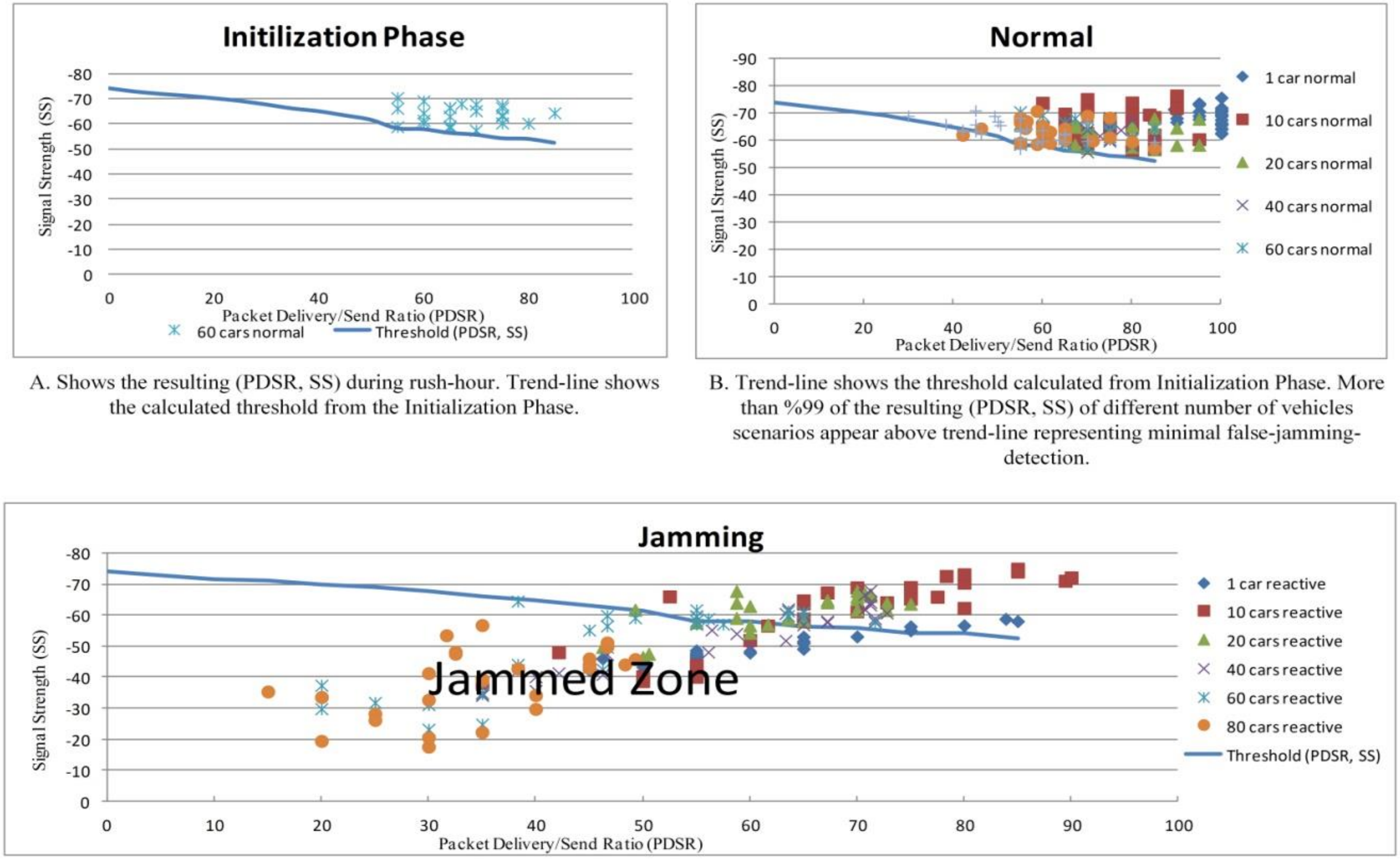
Results Figur.4.1.C shows a strong tie between jammers’ impact (depending on its location) on the measured SS, and the correspondent packet lost rate. In low vehicle density, our algorithm detected jammers when its location is close enough to affect the transmission/delivery of packets. Also, in targeting mobility jamming case, some packets still got delivered correctly depending on the targeted node location and RSU. Additionally, when vehicle density reaches the congestion threshold, RSU detected jammer efficiently once nodes failed to receive sufficient communications based on vehicle density on road. Looking at Fig.4.1, one can clearly see the relation between the observed SS and PDSR in the present and absence of jammers.

4.4 Conclusions

VANET, which is based on inserting wireless access in vehicle environments, are becoming reality and being deployed to enhance safety and provide a variety of services. Although VANET’s main goal is to enhance safety and comfort on roads, intentional jamming aims to undermine such a goal by interfering with the wireless communications. Therefore, understanding the nature of jamming attacks in vehicle environment is critical to ensure the proper operation of the wireless network. This paper has sought to focus on investigating jamming mobility and behaviors in highway roads. We have presented three different jamming behaviors and three mobility patterns that jammer can adopt when launching attacks. We then studied reactive jamming impact, adopting various mobility patterns (stationary, random, or targeting), in different road conditions. We showed jamming effect on PDSR and SS causing failure to receive safety messages. We then proposed a solution to detect jammers based on road conditions in which RSUs are deployed at. Our algorithm proved its effectiveness by achieving high detection accuracy in different vehicle density scenarios.

4.5 SUMMARY

The development of wireless VANET aimed to enhance road's safety and provide comfortable driving environment. This goal can be achieved by ensuring proper dissemination and reception of early warning and infotainment messages. Intentional jamming attack targets at interfering with the normal operation of the network by disrupting wireless communications. Since VANET uses wireless medium as communication mean and performs in outdoor environment (highly changeable road conditions, atmospheric phenomena, and nodes behaviors), estimating the network performance is a challenging task. Due to the nature of VANET, encompasses high mobility of vehicles and volatile topology, applying conventional methods to monitor, analyze and secure the network is infeasible. Thus, we provide this work which focuses jamming mobility and behaviors in IEEE802.11p networks. We focus on analyzing jamming impact, adopting reactive behaviors and different mobility patterns. The combination of various road conditions and random mobility of nodes (traveling speed and directions) makes detecting jamming attacks a challenging task. Thus, to achieve reliable detection, first we identified the impact of vehicles density on the network performance. Then, we studied jamming effectiveness when adopting different mobility patterns (stationary, random, or targeting) and behaviors (constant, random, and reactive). Our three main contributions are, i) Presenting rich contents and details regarding the new technology DSRC and the 802.11p standards, ii) Provide a full understanding of jamming attacks, threats, and capabilities especially when dealing with outdoor wireless networks, and iii) Detecting intentional interference attacks targeting at disrupting the normal operation of IEEE802.11p networks



A. Shows the resulting (PDSR, SS) during rush-hour. Trend-line shows the calculated threshold from the Initialization Phase.

B. Trend-line shows the threshold calculated from Initialization Phase. More than %99 of the resulting (PDSR, SS) of different number of vehicles scenarios appear above trend-line representing minimal false-jamming-detection.

C. Shows the resulting (PDSR, SS) of different scenarios when jammer exist. Trend-line shows the threshold calculated from Initialization Phase. More than %99 of the resulting (PDSR, SS) of different number of vehicles scenarios appear above trend-line representing minimal false-jamming-detection.

Figure.4.1: Result PDSR and SS A) Initialization Phase of 60 cars. B) Normal scenario 1-80 cars. And C) Attacker Scenario 1-80 cars

CHAPTER 5

JAMMING DETECTION – SIMULATION & ANALYSIS

Problem Description & contributions:

1- DSRC uses CCH and SCH. We focus on studying the CCH (Ch178).

2- Study the feasibility to launch jamming attack by transmitting at high fixed power (Constantly or reactively) causing failure to receive packets at the receiver side and consequently a drop in PDR.

3- Proposing a detection algorithm to detect jammers targeting DSRC (dedicated short range communication) in a vehicle network.

WAVE Standards:

1 Nodes: Cars (OBU) + Infrastructure (RSU) introducing V2V and V2X communications with 28.8dBm Max. output power.

2 Channels: 1 Control Channel (Ch 178) with 10 MHz bandwidth and data rate 6Mbps, and 6 Service channels with 10 MHz bandwidth (20Mhz optional) and data rate (3-27Mbps)

3 Channel Access: Control Channel, Service channel, and Guard (5 MHz) – intervals (CCHI, SCHI, GI) was introduced where CCHI and SCHI are roughly = 50µs each, and GI = 1.6 µs (microsecond) as recommended by 1609.4 standards.

4 Messages: Nodes should be able to exchange safety messages on the control channel depending on the incident. The Society of automotive engineers (SAE)-DSRC Tech. Committee has defined in the standards (SAE-J2735) dissemination messages rate at 10 messages/s. They also defined the safety messages size to be (200-500) byte including authentication overhead.

Measurements:

1- BSM: Basic safety messages that is periodically broadcasted to surrounding vehicles.

2- Message Rate: We use the suggested rate of 10 messages per second to broadcast event (safety Msg.)

3- Packet Size: max. reasonable packet size is used (500 byte) for each BSM.

4- PDR: We use packet delivery ratio at the receiver in this analysis. (delivered packets over sent packets)

5- PSR: We use packet sent ratio at sender in this analysis. (sent packets over intended to send)

6- PDSR: This is a new proposed measurement that we will use to evaluate the network behavior. It is intuitive that when Constant jammer exists both PSR and PDR will drop which correspond to low PDSR. On the other hand Reactive jammer will only impact the PDR and hence it is a promising measurement to use to distinguish between different types of jammers.

7- RSSI: We obtain RSSI at the receiver when receiving BSM.

8- SNR: We obtain the signal-to-noise ratio measured at the receiver upon receiving BSM.

9- BER: Bit error rate is obtained at the receiver after decoding the received signals.

10- Throughput: throughput will be used to measure data-flow in channel at all time in Kbps.

Cases: In our work we study 2 main cases, normal and attacker. There are many sub-cases that correspond to the real-life scenarios. We categorize our study cases and sub-cases as follow:

1- Normal cases:

   a. Where vehicle density within 1 RSU range is low enough to produce high PDSR $\left(\frac{PSR}{2} + \frac{PDR}{2}\right)$.

   b. Where vehicle density is high due to congestion and the PDSR will be investigated based on the maximum road's capacity of vehicles depending on the number of lanes.

   Notes: In these cases, we will simulate several scenarios to mimic (interstate and urban) scenarios. Also, nodes density will be tested to find the capacity threshold to ensure the delivery of BSM.

2- Attacker cases:

   a. Attacker is active while vehicle density within 1 RSU range is low.

   b. Attacker is active while vehicle density is high due to congestion (incident).

   Notes: 2 types of attackers will be implemented (constant and reactive) with different mobility behaviors (stationary and mobile).

Performance Analysis (Non Attacker-Highway) scenario: We perform intensive simulations with different node's density to find the node's density threshold that cause high packets drop rate.

Road capacity: in order to build our cases realistically we need to investigate the maximum number of vehicles that can occupy 1 lane in a road. It is worth to mention that we don't consider large vehicles (Trailers, Busses, and semi-trucks), instead we assume that all vehicles are regular size cars. The validity of our assumption is based on the more vehicles occupying roads, the more likely to have congestions. In order to estimate the maximum number of vehicles per lane, we assume that RSU have the maximum communication range up to (1000m) in diameter. Depending on the distance between the RSU and the road we can measure the maximum communication range by drawing a circle around the RSU. Let's assume that RSU can communicate with nodes up to 1000 meter. Therefore the radius of the RSU communication range is 500 denoted (*r*). If the angle (*n*) formed by RSU and road, then the segment area of road that within RSU communication range can be calculated as:

$$\textbf{1 lane Road Segment Area within RSU range} = (r^2 \backslash 2)\ [n\ (\pi/180) - \sin(n)]$$

Where:

n is the central angle in DEGREES

r radius of the circle of which the segment is a part.

π is Pi, approximately 3.142

sin is the trigonometry Sine function

Hence, we can calculate maximum node capacity by dividing the calculated segment over vehicle node dimension. (Average 4meter length x 2 meter width –Full size cars) we add 4 meters in length to compensate for space required between cars in front and behind (since stacking cars bumper to bumper is not feasible). Hence an average dimension for cars (excluding trucks and irregular car sizes) should occupy an area of 12 m^2. Therefore, the maximum road capacity of vehicles within RSU range will be:

$$\underline{\mathbf{Max\ Capacity = (r^2\backslash 2)\ [\ n(\pi/180)\text{-}\sin n]\ /\ [(L+S)*W]}}$$

L: vehicle length.
S: space between nodes.
W: cars width.

We assume that RSU is sitting at the edge of the road for simplicity, then the value of *n* (the angle between RSU and the edge of the road on both sides of that RSU is 180^o. Hence the maximum number of vehicles that can occupy <u>one lane</u> within an RSU range of (1000m) will be:

= approximately 110 regular size vehicles.

Alternatively, we use a simpler technique that is based on the road length (1000m) and divide that over the average length of vehicles (6 m). We also add 4 m to the vehicle's length to compensate for the safe distance behind and in-front of vehicles as follow:

Road to vehicles capacity = 1000 / [6+4]

We use the value (<u>100 as the upper bound)</u> to correspond to the maximum road's capacity of vehicles. when evaluating the network behavior in the simulator platform.

<u>Propagation model:</u> We use *free space and shadowing* propagation model since in a real world RSU may be deployed in an area where there exist LoS between RSU and vehicles.

Fading model: 2 fading models were investigated (raician and rayligh). Due to the possibility of LoS existence between nodes we use Raician model in our simulations since Rician fading occurs when one of the paths, typically a LoS, is much stronger than the others.

Simulation time: Due to the numerous numbers of cases and scenarios that we will simulate, we need to carefully choose simulation time that will be large enough to collect necessary data and short enough to avoid unnecessary processing and resources usage. Hence, we investigate the simulation time that we need for that matter. Let's assume cars travelling in an interstate (speed [45-80mph]). Hence in order to capture communications data between nodes and RSU (when entering, driving, and exiting RSU communication range), we define our simulation time to be the time that is needed for high speed vehicles to enter and exit RSU communication range. Hence the simulation time can be calculated as follow:

Simulation time = RSU max communication range / vehicles maximum speed

= 1000m / 80Mph = 1000m / 35 mps = 28.5 seconds

Therefore, we use 30 seconds to be our simulation time to compensate for vehicles entering and exiting RSU communication range, and save computer resources during simulations.

Link availability time: Based on current study, link availability in mobile network depends entirely (in general) on the distance between sender and receiver. So we consider the link availability between nodes based on the distance between node and RSU. Hence we can define the link availability between RSU and any vehicle node to be AVAILABLE_Link for time (*t in seconds*) where *t* is the time from car node enter RSU communication range until existing RSU range (which is a function of car speed and the distance between RSU and car node).

Simulation Parameters:

The table below summarizes our general simulation parameters:

Table 5.1: Simulation Parameters

Parameter	Value	Notes
Simulator	NCTUns	Release 6.0
Simulation Time	30 seconds	Per simulation case
Node Type	RSU & OBU	-----
Topology	Interstate & Urban	-----
Minimum number of vehicles	1	-----
Maximum Number of vehicles	110	Per lane
Mobile node speed	(45-80) or (20-50) Mph	Interstate vs. Urban
Acceleration, Deceleration	Freely	Car nodes
Number of lanes (bi-direction)	2	1lane each direction
Lane width	4 m	US regulation
Channel Type	Control Channel	-----
Channel Number	178	-----
Channel Frequency	5.890 GHz	5.885-5.895 Ghz
Channel spacing (bandwidth)	10 Mhz	-----
Channel Interval	50 ms	-----
Propagation	Free space and shadowing	-----
Fading Model	Rician	-----
Data Type	BSM	Basic Safety Message
BSM (Packet) size	500 byte	1 BSM per packet
Communication type	Broadcast	Bi-directional (V2X)
RSU-BSM rate	10 messages per second	US Standards
Car-BSM rate	10 messages per second	Correspond to incident
Data rate (CCH)	6 Mbps	Standards Recommendation (CCH)
Max. Transmission power	28.8 dbm	Standards
Receiver sensitivity	-82	-----
Transport layer protocol	UDP	Standards Recommendation

Topology (Interstate):

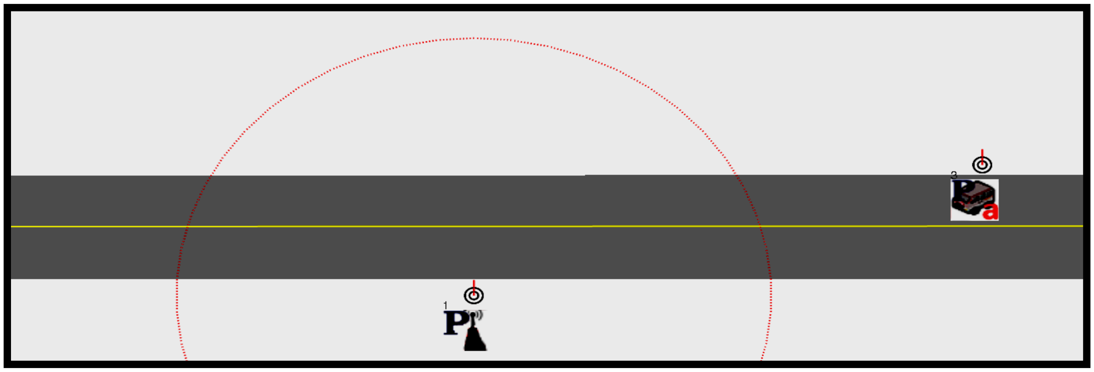


Figure 5.1: Highway Topology

Normal-Case1 (1 RSU + 1 Car)

In this case, we simulate 1 Car and 1 RSU exchanging 10 BSM/s at 500 byte/BSM using broadcasting technique in an interstate topology where car speed is between 45-80 Mph. Each node (Car or RSU) will be broadcasting 10 messages per second where each message is transmitted as UDP packet at size of 500 byte per message.

Results: after collecting results, we notice the accumulated packets lost are 30 packets out of total 300 packets transmitted. I.e. out of the 300 BSM that was sent by RSU, car moving at high speed was able to receive 260 messages during driving in that RSU range.

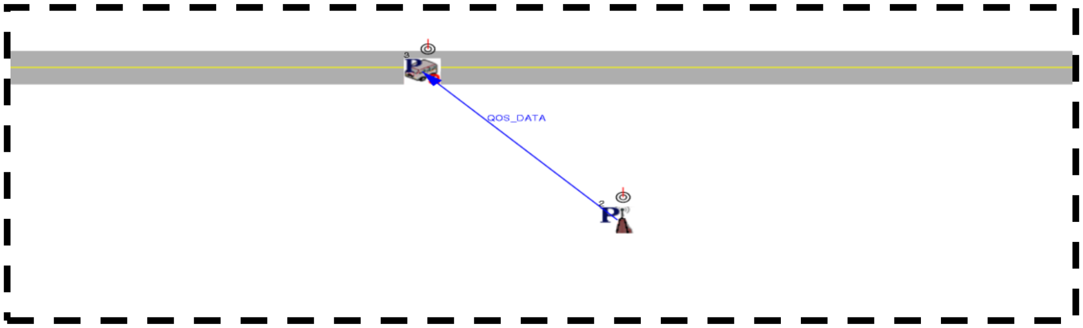


Figure 5.2: 1 OBU and 1 RSU Highway Scenario

Normal-Case 2 (1 RSU + 10 Cars):

In this case, we simulate 10 Cars and 1 RSU exchanging 10 BSM/s at 500 byte/BSM using broadcasting technique in an interstate topology where cars speed is between 45-80 Mph. Each node (Car or RSU) will be broadcasting 10 messages per second where each message is transmitted as UDP packet at size of 500 byte per message.

Results: after collecting results, we notice the accumulated packets lost are 144 packets out of total 300 packets transmitted by RSU.

In other word, out of the 300 BSM (30 unique safety messages) that was sent by RSU, car moving at high speed was able to receive 156 messages during driving in that RSU range. We also note that Cars will still receive all the messages that RSU transmitted even though the presence of 9 more vehicles travelling on the same route resulted on higher packets loss.

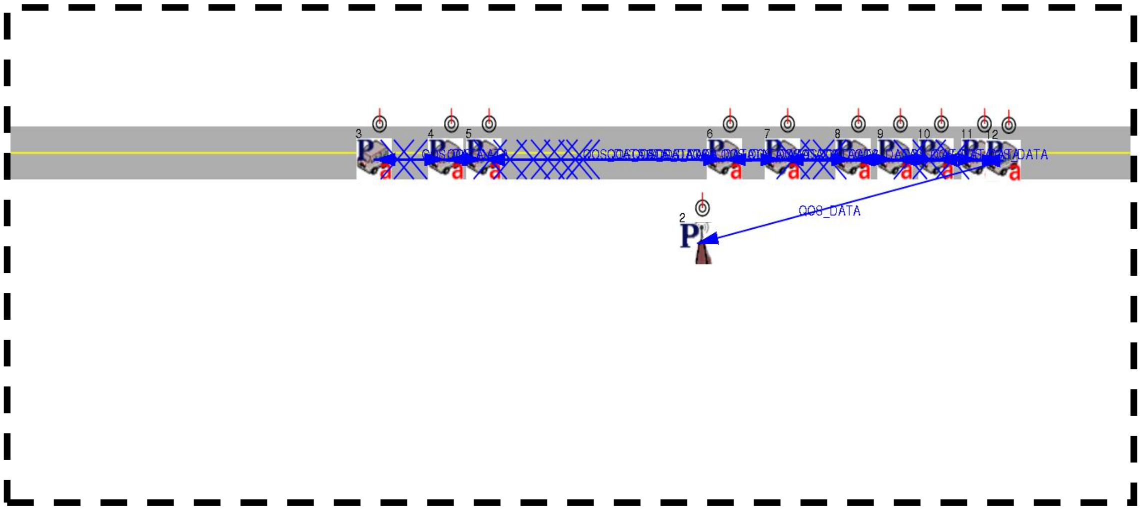


Figure 5.3: 10 OBUs and 1 RSU Highway Scenario

Normal-Case 3 (1 RSU + 20 Cars):

In this case, we simulate 20 Cars and 1 RSU exchanging 10 BSM/s at 500 byte/BSM using broadcasting technique in an interstate topology where cars speed is between 45-80 Mph. Each node (Car or RSU) will be broadcasting 10 messages per second where each message is transmitted as UDP packet at size of 500 byte per message.

Results: after collecting results, we notice the accumulated packets lost are 155 packets out of total 300 packets transmitted by RSU.

In other word, out of the 300 BSM (30 unique safety messages) that was sent by RSU, car moving at high speed was able to receive 145 messages during driving in that RSU range. We also note that Cars were still able to receive more than 1BSM/sec RSU transmitted even though the presence of 19 more vehicles travelling on the same route resulted on higher packets loss.

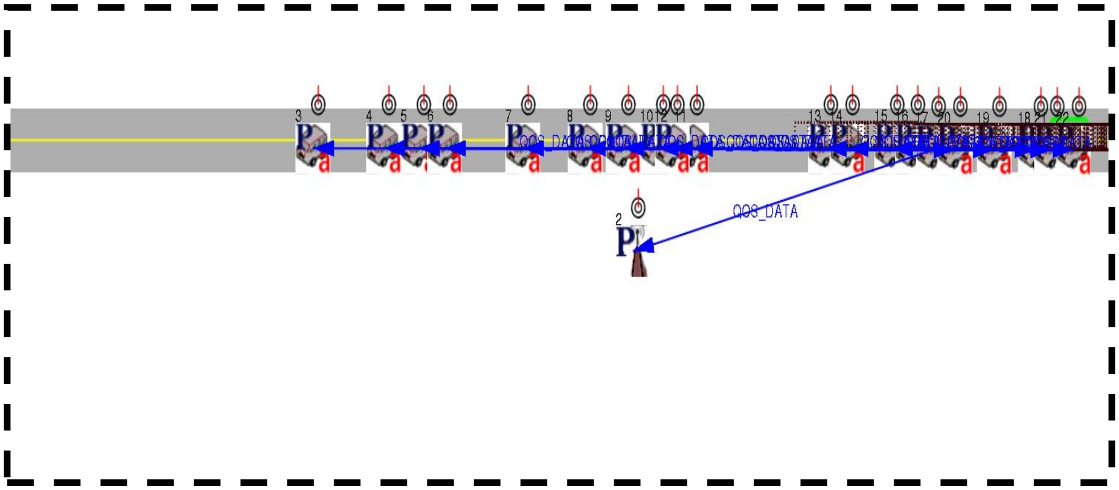


Figure 5.4: 20 OBUs and 1 RSU Highway Scenario

Normal-Case 4 (1 RSU + 40 Cars):

In this case, we simulate 40 Cars and 1 RSU exchanging 10 BSM/s at 500 byte/BSM using broadcasting technique in an interstate topology where cars speed is between 45-80 Mph. Each node (Car or RSU) will be broadcasting 10 messages per second where each message is transmitted as UDP packet at size of 500 byte per message.

Results: after collecting results, we notice the accumulated packets lost are 183 packets out of total 300 packets transmitted by RSU.

In other word, out of the 300 BSM (30 unique safety messages) that was sent by RSU, car moving at high speed was able to receive 117 messages during driving in that RSU range. We also note that Cars (overall) were still able to receive more than 1BSM/second that RSU transmitted even though the presence of 39 more vehicles travelling on the same route resulted on higher packets loss.

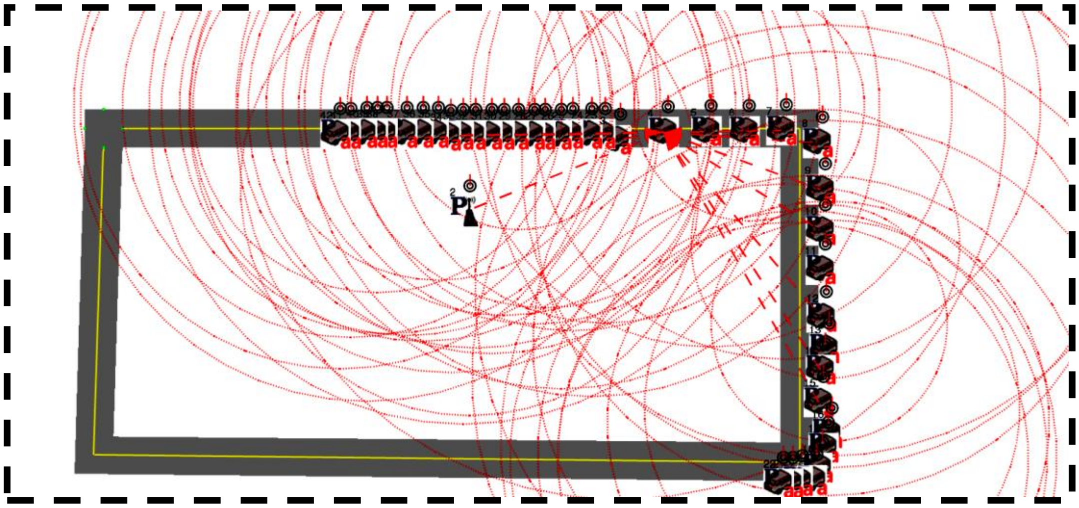


Figure 5.5: 40 OBUs and 1 RSU Highway Scenario

Normal-Case 5 (1 RSU + 60 Cars):

In this case, we simulate 60 Cars and 1 RSU exchanging 10 BSM/s at 500 byte/BSM using broadcasting technique in an interstate topology where cars speed is between 45-80 Mph. Each node (Car or RSU) will be broadcasting 10 messages per second where each message is transmitted as UDP packet at size of 500 byte per message.

Results: after collecting results, we notice the accumulated packets lost are 197 packets out of total 300 packets transmitted by RSU.

In other word, out of the 300 BSM (30 unique safety messages) that was sent by RSU, car moving at high speed was able to receive 103 messages during driving in that RSU range. We also note that Cars still were able to receive all the messages that RSU transmitted even though the presence of 59 more vehicles travelling on the same route resulted on higher packets loss.

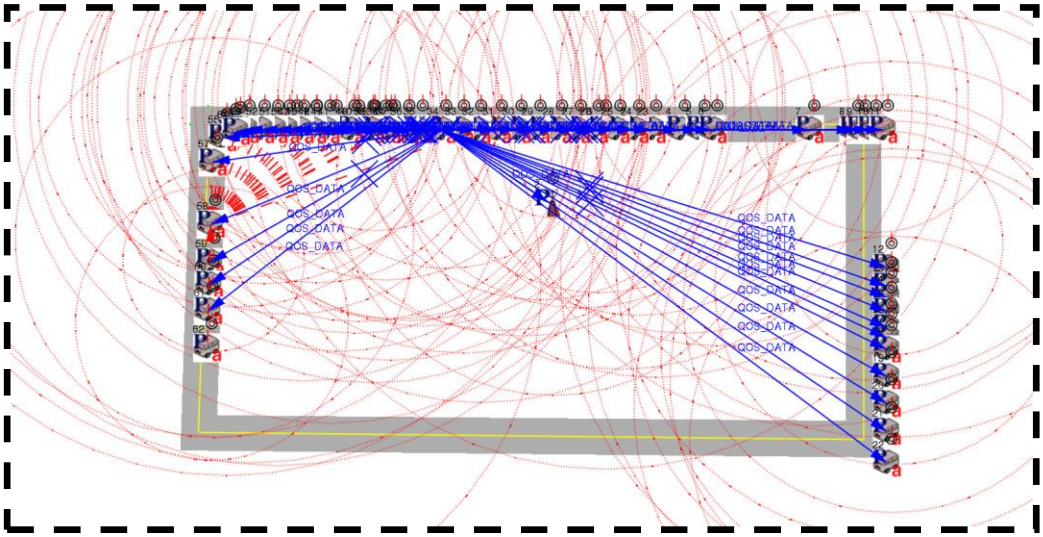


Figure 5.6: 60 OBUs and 1 RSU Highway Scenario

Normal-Case 6 (1 RSU + 80 Cars):

In this case, we simulate 80 Cars and 1 RSU exchanging 10 BSM/s at 500 byte/BSM using broadcasting technique in an interstate topology where cars speed is between 45-80 Mph. Each node (Car or RSU) will be broadcasting 10 messages per second where each message is transmitted as UDP packet at size of 500 byte per message.

Results: after collecting results, we notice the accumulated packets lost are 215 packets out of total 300 packets transmitted by RSU.

Conclusion: In other word, out of the 300 BSM (30 unique safety messages) that was sent by RSU, car moving at high speed was able to receive 85 messages during driving in that RSU range. We also note that Cars still were able to receive all the messages (at least 1 BSM/s) that RSU transmitted even though the presence of 79 more vehicles travelling on the same route resulted on higher packets loss.

Normal-Case 7 (1 RSU + 100 Cars):

In this case, we simulate 100 Cars and 1 RSU exchanging 10 BSM/s at 500 byte/BSM using broadcasting technique in an interstate topology where cars speed is between 45-80 Mph. Each node (Car or RSU) will be broadcasting 10 messages per second where each message is transmitted as UDP packet at size of 500 byte per message.

Results: after collecting results, we notice the accumulated packets lost are 247 packets out of total 300 packets transmitted by RSU.

Conclusion: In other words, out of the 300 BSM (30 unique safety messages) that was sent by RSU, car moving at high speed was able to receive 53 messages during driving in that

RSU range (only 24 unique BSMs were received). We also note that when nodes density reaches 100 nodes within 1 RSU range, the channel bandwidth is unable to sustain nodes congestions and hence safety messages will be lost.

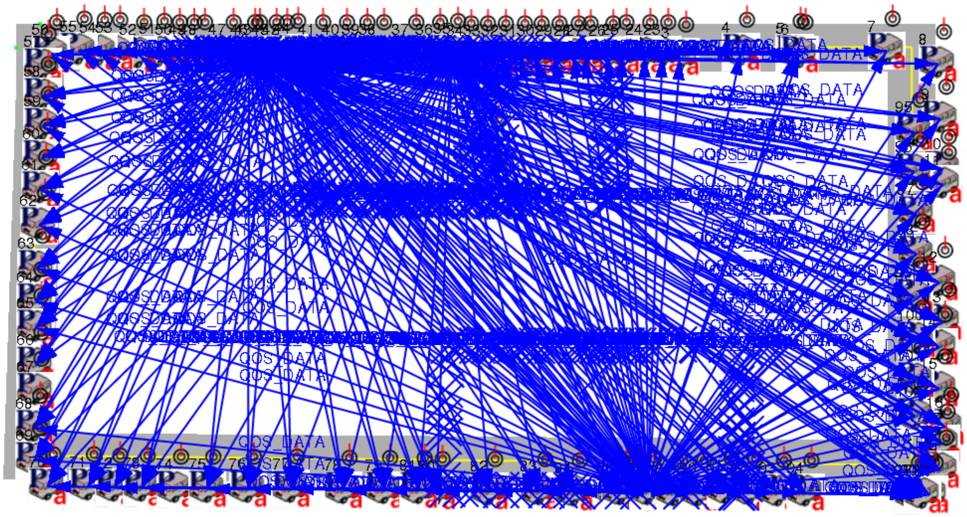


Figure 5.7: 100 OBUs and 1 RSU Highway Scenario

Further Notes:

We noticed that most of packets got lost due to the impact of node's density on RSU communication (hearing) range. In other words, the higher cars density within RSU range, the higher attenuation occurs in nodes hearing range within that area due to the increase in the noise power. Also, in an area where nodes density is high, the probability of packets to collide is high which explain the drastic drop in packet delivery ratio. We notice that there exist a tight relationship between RSU's and cars communication range, and vehicles density within that area at time t. In other words, there is a tradeoff between the number of vehicles in any section of the road and the communication range of all nodes existed in that area. So, we relate the increase of packet loss to the increase of cars density within an RSU range which impact communication range and the collision probability between packets.

We also noticed that in highway scenarios when nodes density increases the cars speed decreases and hence the link-availability-duration increase because cars will spend longer time within the RSU range. Although this should increase the probability for vehicles to receive messages correctly however, depending on the number of vehicles that may exist during congestion, communication overhead may occur consequently causing attenuation to communication range between nodes.

RSU Deployment Location:

In our analysis we discussed how nodes density affects the number of dropped packets. Hence, we propose placing RSU in away to have a maximum node's density of no more than 90 nodes per lane (to ensure the delivery of at least 1 BSM/s).

Recall the formula which calculates the maximum number of vehicles that can occupy 1 lane.

Max Capacity\ 1 lane = (r^2\2) [n(π/180)-sin n] / [(L+S)*W]

Then we can use it to find the best location to deploy RSUs based on their distance from road as follow:

90 = 125000 [n(π)/180) – Sin n] / [L+S) * W

90 = 500 [n (π) / 180 – Sin n] / 12

n (π) – Sin n = approx. 400 meter between RSUs when deploy

Hence, RSU (with high vehicles density within its communication range) can communicate up to approximately 400* 2 = 800 meter if it was sitting at the edge of the road.

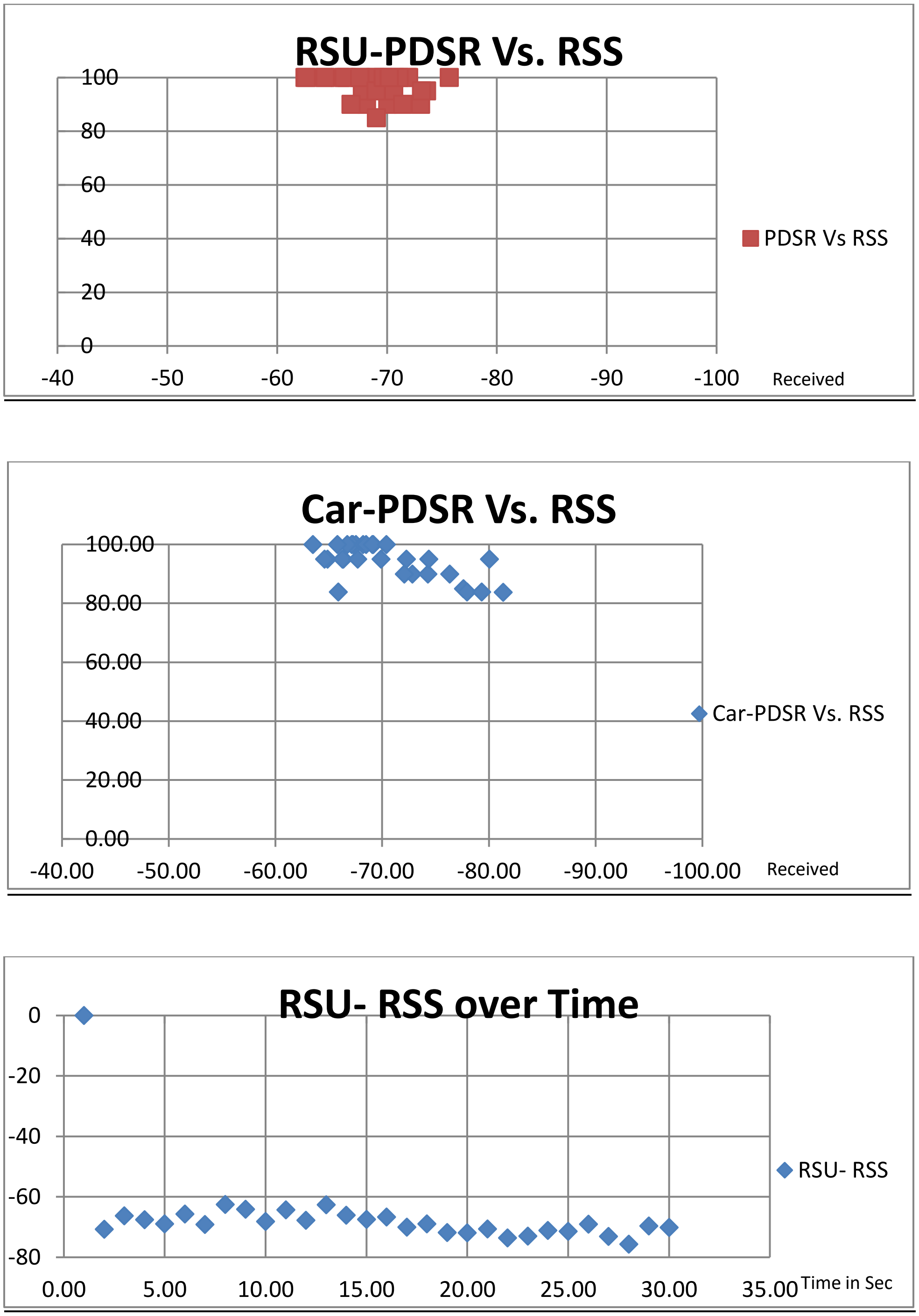


Figure 5.8 20 OBUs + 1 RSU (non-attacker):

60 OBU + 1 RSU (non-attacker)

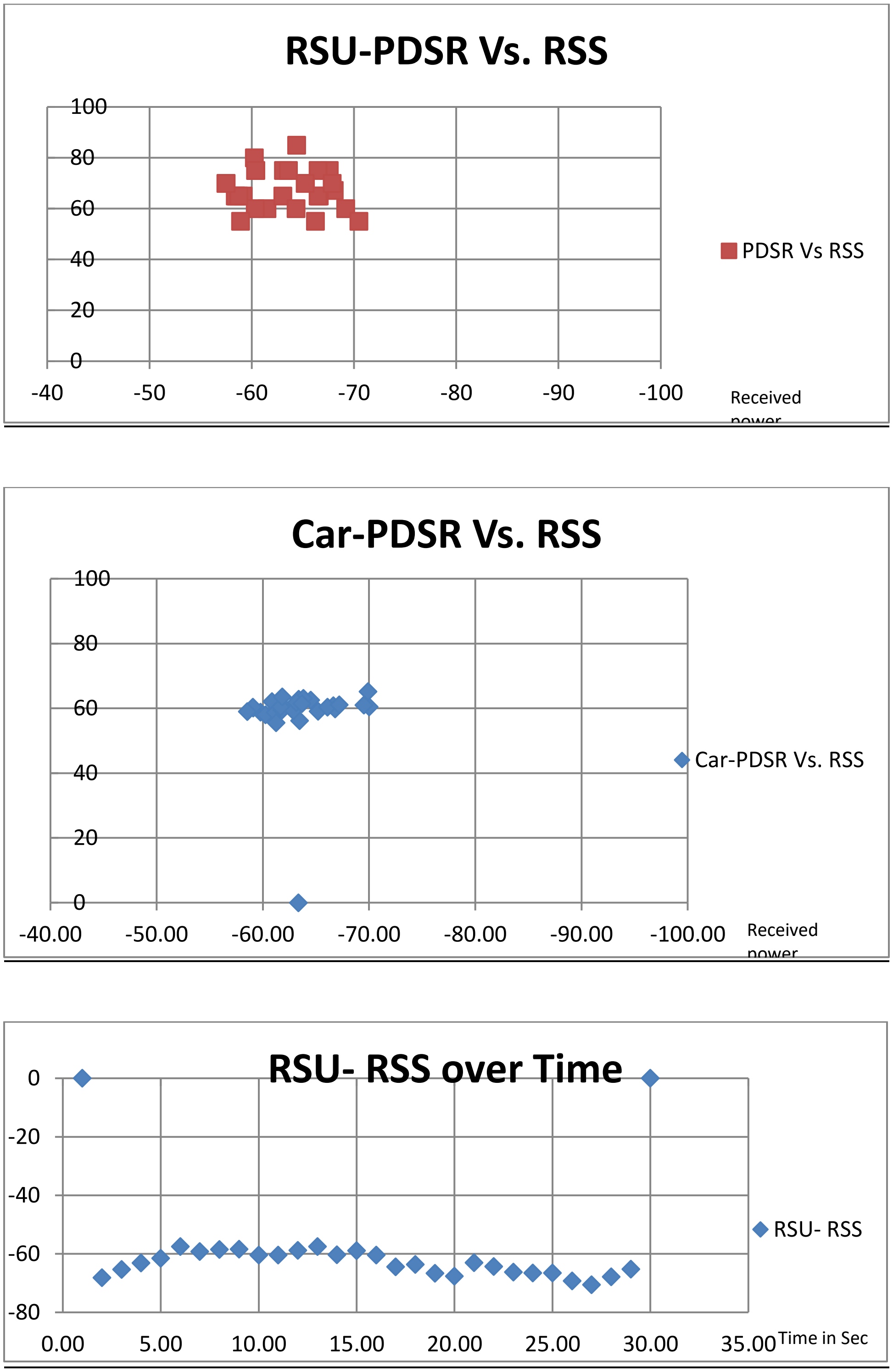


Figure 5.9: 60 OBUs + 1 RSU (non-attacker)

100 OBU + 1 RSU (non-attacker)

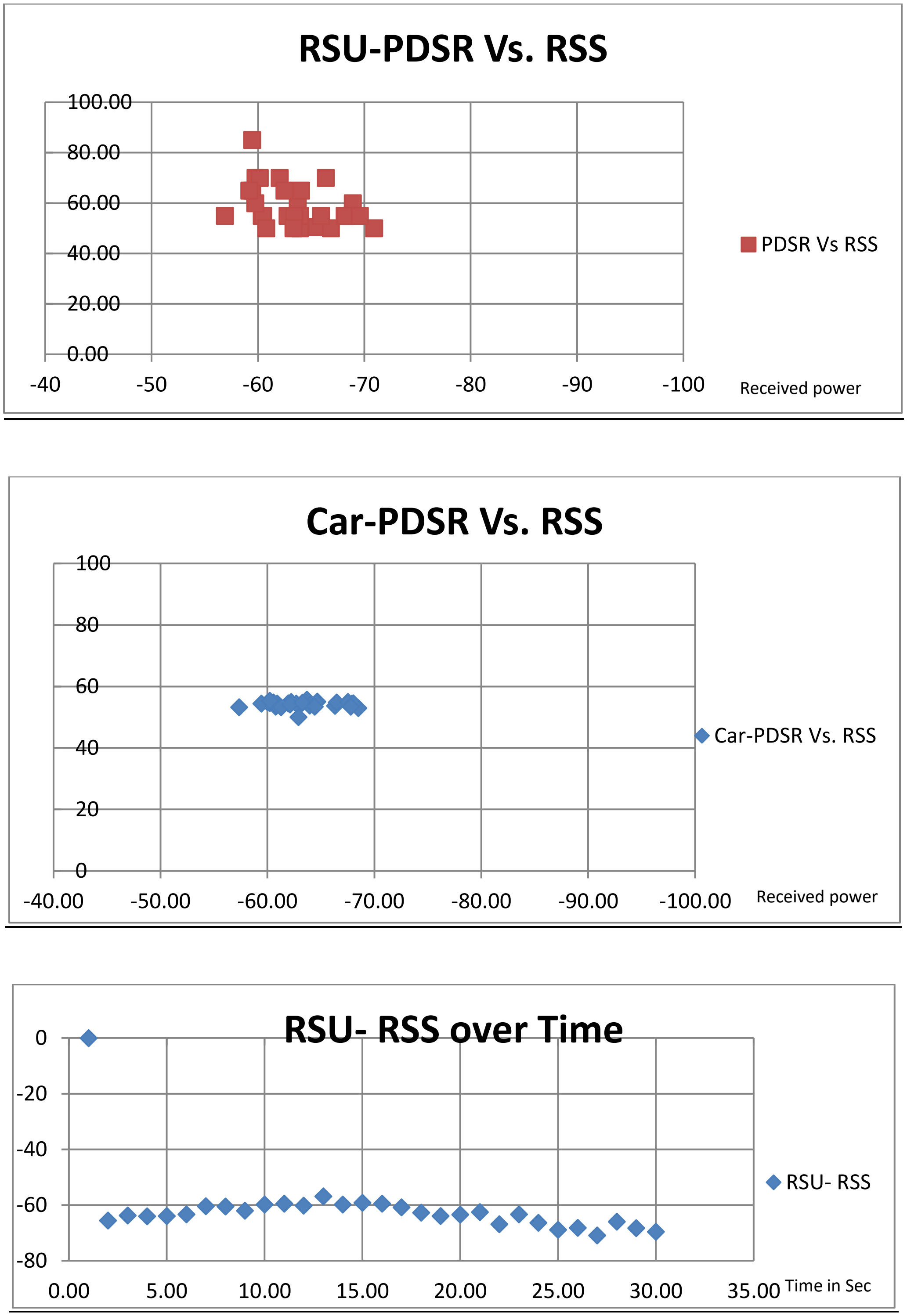


Figure 5.10:100 OBUs + 1 RSU (non-attacker)

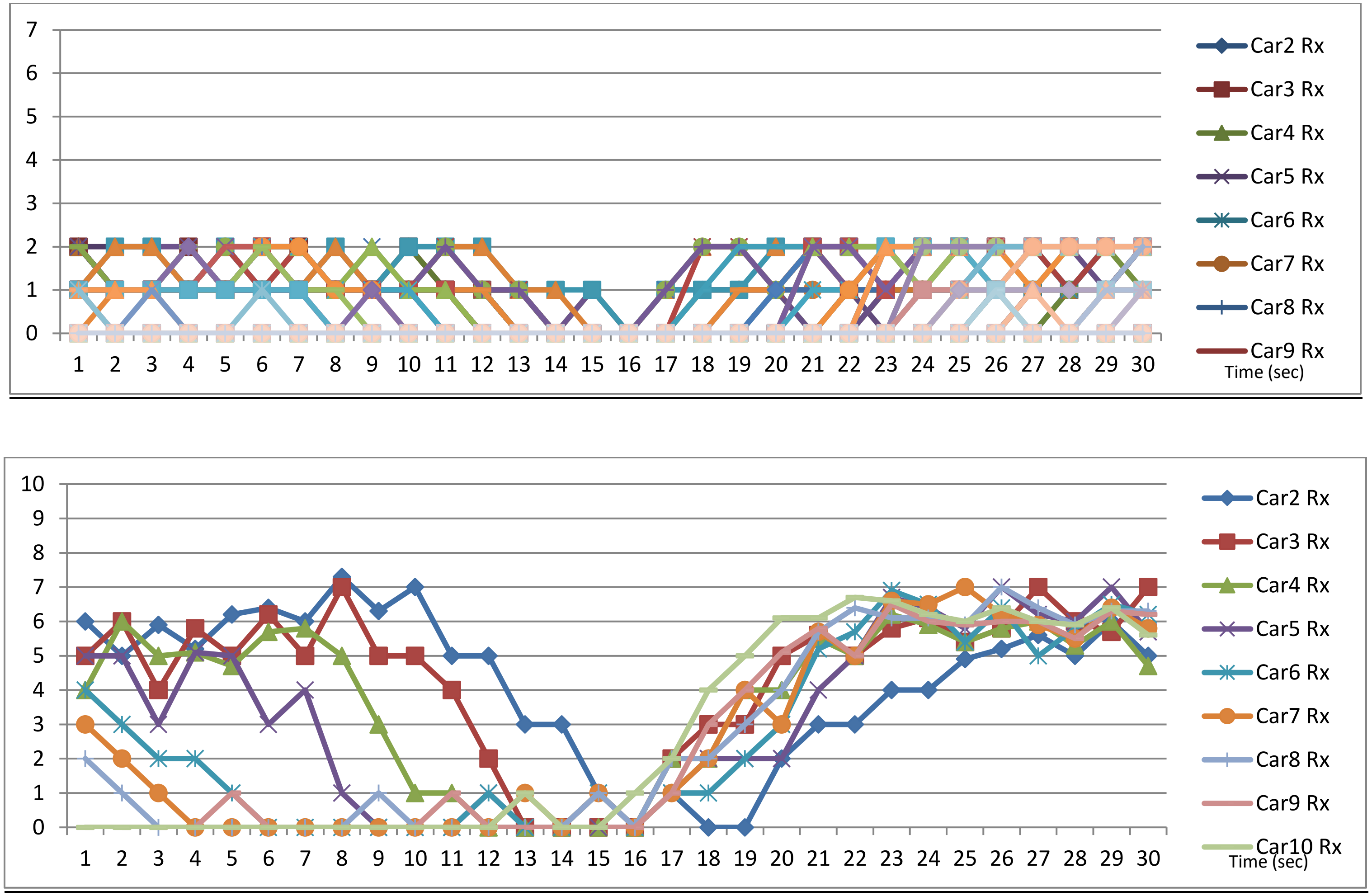
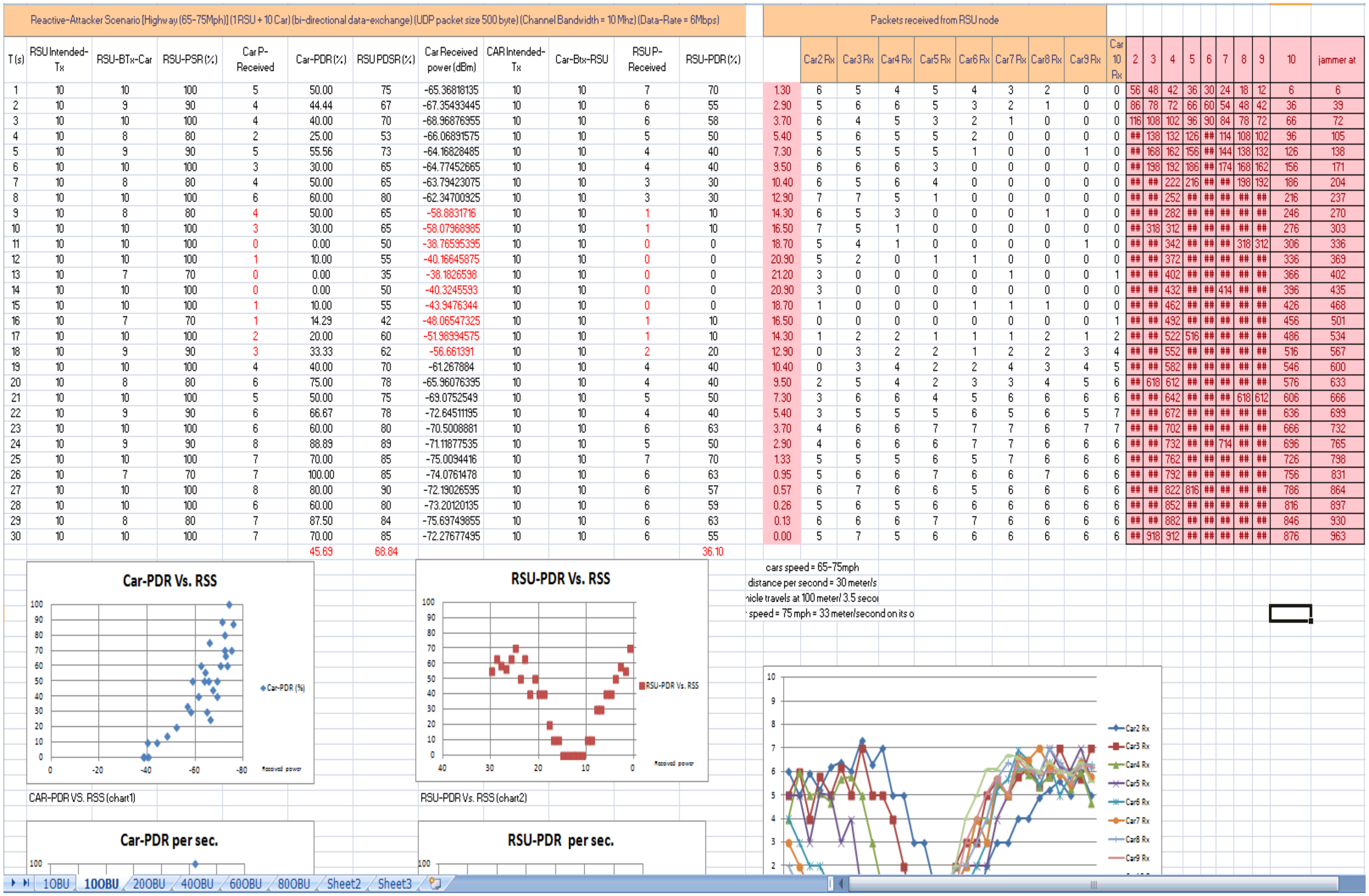


Figure 5.11: Reactive jammer impact on exchanging BSMs



Reactive-Attacker Scenario [Highway (65-75Mph)] (1 RSU + 10 Car) (bi-directional data-exchange) (UDP packet size 500 byte) (Channel Bandwidth = 10 Mhz) (Data-Rate = 6Mbps)											
T (s)	RSU Intended-Tx	RSU-BTx-Car	RSU-PSR (%)	Car P-Received	Car-PDR (%)	RSU PDSR (%)	Car Received power (dBm)	CAR Intended-Tx	Car-Btx-RSU	RSU P-Received	RSU-PDR (%)
1	10	10	100	5	50.00	75	-65.36818135	10	10	7	70
2	10	9	90	4	44.44	67	-67.35493445	10	10	6	55
3	10	10	100	4	40.00	70	-68.96876955	10	10	6	58
4	10	8	80	2	25.00	53	-66.06891575	10	10	5	50
5	10	9	90	5	55.56	73	-64.16828485	10	10	4	40
6	10	10	100	3	30.00	65	-64.77452665	10	10	4	40
7	10	8	80	4	50.00	65	-63.79423075	10	10	3	30
8	10	10	100	6	60.00	80	-62.34700925	10	10	3	30
9	10	8	80	4	50.00	65	-58.8831716	10	10	1	10
10	10	10	100	3	30.00	65	-58.07968985	10	10	1	10
11	10	10	100	0	0.00	50	-38.76595395	10	10	0	0
12	10	10	100	1	10.00	55	-40.16645875	10	10	0	0
13	10	7	70	0	0.00	35	-38.1826598	10	10	0	0
14	10	10	100	0	0.00	50	-40.3245593	10	10	0	0
15	10	10	100	1	10.00	55	-43.9476344	10	10	0	0
16	10	7	70	1	14.29	42	-48.06547325	10	10	1	10
17	10	10	100	2	20.00	60	-51.98994575	10	10	1	10
18	10	9	90	3	33.33	62	-56.661391	10	10	2	20
19	10	10	100	4	40.00	70	-61.267884	10	10	4	40
20	10	8	80	6	75.00	78	-65.96076395	10	10	4	40
21	10	10	100	5	50.00	75	-69.0752549	10	10	5	50
22	10	9	90	6	66.67	78	-72.64511195	10	10	4	40
23	10	10	100	6	60.00	80	-70.5008881	10	10	6	63
24	10	9	90	8	88.89	89	-71.11877535	10	10	5	50
25	10	10	100	7	70.00	85	-75.0094416	10	10	7	70
26	10	7	70	7	100.00	85	-74.0761478	10	10	6	63
27	10	10	100	8	80.00	90	-72.19026595	10	10	6	57
28	10	10	100	6	60.00	80	-73.20120135	10	10	6	59
29	10	8	80	7	87.50	84	-75.69749855	10	10	6	63
30	10	10	100	7	70.00	85	-72.27677495	10	10	6	55
					45.69	68.84					36.10

T (s)		Packets received from RSU node																		
		Car2 Rx	Car3 Rx	Car4 Rx	Car5 Rx	Car6 Rx	Car7 Rx	Car8 Rx	Car9 Rx	Car 10 Rx	2	3	4	5	6	7	8	9	10	jammer at
1	1.30	6	5	4	5	4	3	2	0	0	56	48	42	36	30	24	18	12	6	6
2	2.90	5	6	6	5	3	2	1	0	0	86	78	72	66	60	54	48	42	36	39
3	3.70	6	4	5	3	2	1	0	0	0	116	108	102	96	90	84	78	72	66	72
4	5.40	5	6	5	5	2	0	0	0	0	##	138	132	126	##	114	108	102	96	105
5	7.30	6	5	5	5	1	0	0	1	0	##	168	162	156	##	144	138	132	126	138
6	9.50	6	6	6	3	0	0	0	0	0	##	198	192	186	##	174	168	162	156	171
7	10.40	6	5	6	4	0	0	0	0	0	##	##	222	216	##	##	198	192	186	204
8	12.90	7	7	5	1	0	0	0	0	0	##	##	252	##	##	##	##	##	216	237
9	14.30	6	5	3	0	0	0	1	0	0	##	##	282	##	##	##	##	##	246	270
10	16.50	7	5	1	0	0	0	0	0	0	##	318	312	##	##	##	##	##	276	303
11	18.70	5	4	1	0	0	0	0	1	0	##	##	342	##	##	##	318	312	306	336
12	20.90	5	2	0	1	1	0	0	0	0	##	##	372	##	##	##	##	##	336	369
13	21.20	3	0	0	0	0	1	0	0	1	##	##	402	##	##	##	##	##	366	402
14	20.90	3	0	0	0	0	0	0	0	0	##	##	432	##	##	414	##	##	396	435
15	18.70	1	0	0	0	1	1	1	0	0	##	##	462	##	##	##	##	##	426	468
16	16.50	0	0	0	0	0	0	0	0	1	##	##	492	##	##	##	##	##	456	501
17	14.30	1	2	2	1	1	1	2	1	2	##	##	522	516	##	##	##	##	486	534
18	12.90	0	3	2	2	1	2	2	3	4	##	##	552	##	##	##	##	##	516	567
19	10.40	0	3	4	2	2	4	3	4	5	##	##	582	##	##	##	##	##	546	600
20	9.50	2	5	4	2	3	3	4	5	6	##	618	612	##	##	##	##	##	576	633
21	7.30	3	6	6	4	5	6	6	6	6	##	##	642	##	##	##	618	612	606	666
22	5.40	3	5	5	5	6	5	6	5	7	##	##	672	##	##	##	##	##	636	699
23	3.70	4	6	6	7	7	7	6	7	7	##	##	702	##	##	##	##	##	666	732
24	2.90	4	6	6	6	7	7	6	6	6	##	##	732	##	##	714	##	##	696	765
25	1.33	5	5	5	6	5	7	6	6	6	##	##	762	##	##	##	##	##	726	798
26	0.95	5	6	6	7	6	6	7	6	6	##	##	792	##	##	##	##	##	756	831
27	0.57	6	7	6	6	5	6	6	6	6	##	##	822	816	##	##	##	##	786	864
28	0.26	5	6	5	6	6	6	6	6	6	##	##	852	##	##	##	##	##	816	897
29	0.13	6	6	6	7	7	6	6	6	6	##	##	882	##	##	##	##	##	846	930
30	0.00	5	7	5	6	6	6	6	6	6	##	918	912	##	##	##	##	##	876	963

cars speed = 65-75mph
distance per second = 30 meter/s
nicle travels at 100 meter/ 3.5 secoı
speed = 75 mph = 33 meter/second on its o

CAR-PDR VS. RSS (chart1)

RSU-PDR Vs. RSS (chart2)

Figure 5.12: Sample Data after cleaning

CHAPTER 6

Experimental Analysis of Long-Range Radio Communications Capabilities Among Multiple Autonomous Surface Vehicles (ASVs)

The rapid advancement in sensor modalities enabled a fleet of robots to carry their missions autonomously and efficiently and by maintaining reliable communications among them and base-stations [58]. Although robots nowadays are more sophisticated in term of exploring capability (drive, fly, and dive autonomously) based on sensory data, monitoring exploring robots during A mission is crucial to minimize potential loss (fatality or financially). Hence, it is essential to provide low latency, reliable, and robust communication channels to ensure a continuous and effective monitoring of autonomous robots during missions. The desirable communication range along with the number of communicating nodes, are the key factors that define the frequency band (VHF, UHF, SHF, etc.) To be used in the radio spectrum for communications. Nevertheless, several other factors contribute to degrading the quality of communications, such as, but not limited to, environmental noise and weather outdoor, and walls and obstacles indoor.

6.1 Introduction, Literature, and Motivations.

Several works investigated the wireless communications among a fleet of autonomous vehicles and provided a rich analysis in different communication bands of the rf spectrum. Hayat et al. [59] demonstrated in their work the feasibility of maintaining links between multiple drones and base station in single/multi-hop manner. Although their work showed promising results by adopting the wi-fi band for communications (802.11N, ac), communicating in wi-fi band is limited in range up to a couple of hundred meters [60]. Also, Morgenthaler et al. Developed the UAVNET prototype that forms a flying wireless mesh network [61]. Results showed 6.3 times higher throughput in flying wireless mesh nodes than a ground-based network approach.

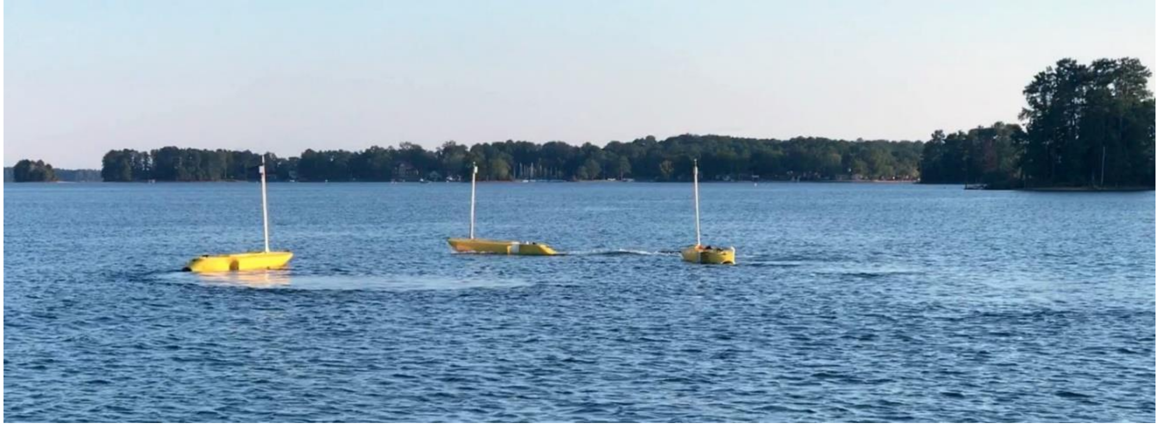


Figure. 6.1: Jetyaks equipped with RFD900+ modems

This chapter presents a performance evaluation that can be used as a guide to understand the capability and reliability of long range communications. Such a study can then be used to better design a network for a team of multiple robots in marine environments, where long range distance communication is necessary. We present the different configurations that can be setup and their impacts on communications in a mobile environment. We focus on communicating in the ism band (900MHz) when experimenting indoor and outdoor. We use cheap, off the Shelf radio frequency (rf) modems – open source RFD900+ (widely used for peer-to-peer telemetry communications). Several indoor and outdoor experiments show the quality of the communications in terms of latency, range, and the impact on data rate and RSSI value (received signal strength indicator). It is worth mentioning that our motive behind adopting 900 MHz is the low-cost/weight of the hardware, and the potential to cover longer ranges with better penetration through obstacles than higher frequencies. Due to limited space when running indoor experiments, we assume stationary robots. More significantly, outdoor experiments were conducted by mounting rfd900+ hardware on a fleet of autonomous surface vehicles (ASV) masts; see fig.6.1. We present multiple setup scenarios and discussions regarding the radio configuration and results. We start by evaluating the communication between one base station and one mobile robot. Results show that we can maintain robust link between the Jetyaks and bs (base-station). We then add another bs to simulate multiple BSs monitoring the same Jetyak. Several other key-experiments were performed with multiple Jetyaks communicating with multiple BSs forming a mesh-like network. Observations and analysis are discussed related to evaluating communication links between multiple Jetyaks and BSs. Fig. 6.2 shows a deployment in the Congaree river in South Carolina with four Jetyaks, where the communication quality was experimentally evaluated fig. 6.3. The main contribution is to give an insight of the different setups that can be easily adopted when monitoring autonomous vehicles over a long range (over 10 miles) using basic hardware and how to optimize and tune parameters to achieve higher throughput and range. Future work will consider the construction of a communication map [62] in order to control the ASVs facilitating a communication link to the ground control station while Exploring areas larger than the communication ranges [63].

6.2 Experimental Setup and case-studies

We conducted multiple experiments indoors and outdoors using RFD900+ radio modem fig 6.4 to evaluate the quality of communications of 900MHz band. We also ran multiple scenarios for each experiment where two nodes were communicating with each other as a base station and remote node. We then added another remote node to analyze the impact on the quality of communications. All indoor experiments were run in the Horizon II building were base station was installed in one room in the first floor (#1215) and remote node in another room (#1205). The distance between the two rooms were at least 150 ft. with, multiple walls exist in between (more than 8 walls) to test the penetration strength of the signal. Table 6.1 shows the various parameters that can be configured when setting up nodes for communications. On the other hand, all outdoor experiments were conducted on either Lake Murray or the Congaree river where Jetyaks were either controlled by a transmitter or an actual personnel riding in them. Fig 5.5 shows the preparation for one of the outdoor experiment on the Congaree River.

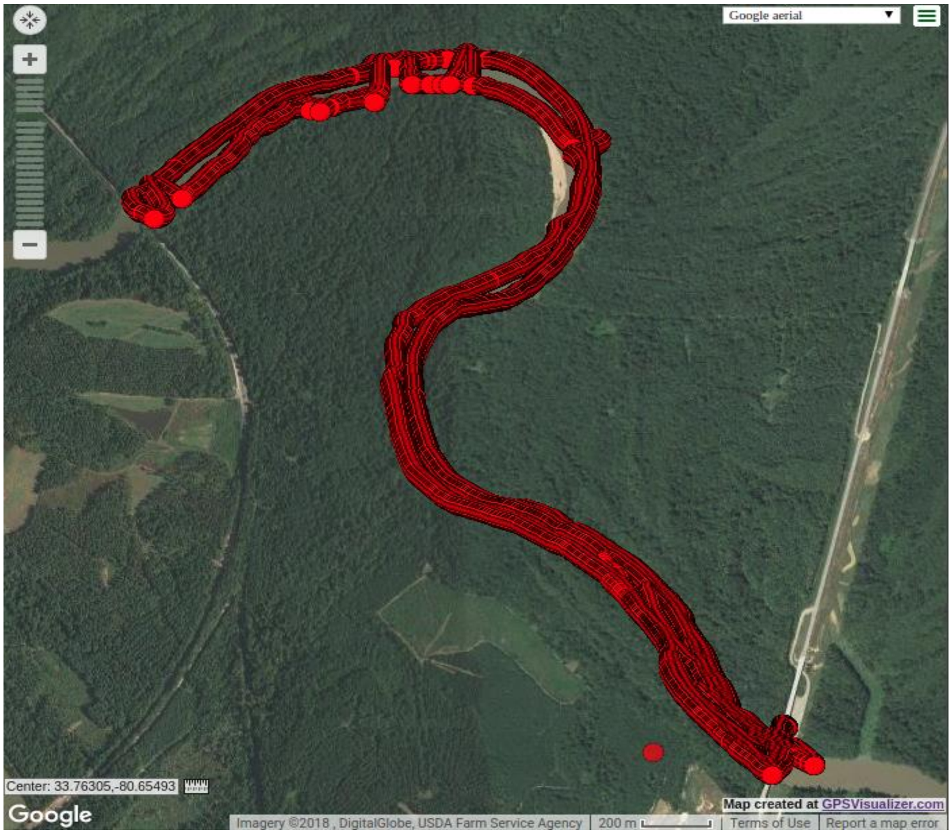

Google aerial
Center: 33.76305,-80.65493
Google
Map created at GPSVisualizer.com
Imagery ©2018 , DigitalGlobe, USDA Farm Service Agency
200 m
Terms of Use
Report a map error

Figure 6.2: GPS traces of four ASVs during deployment at the Congaree River

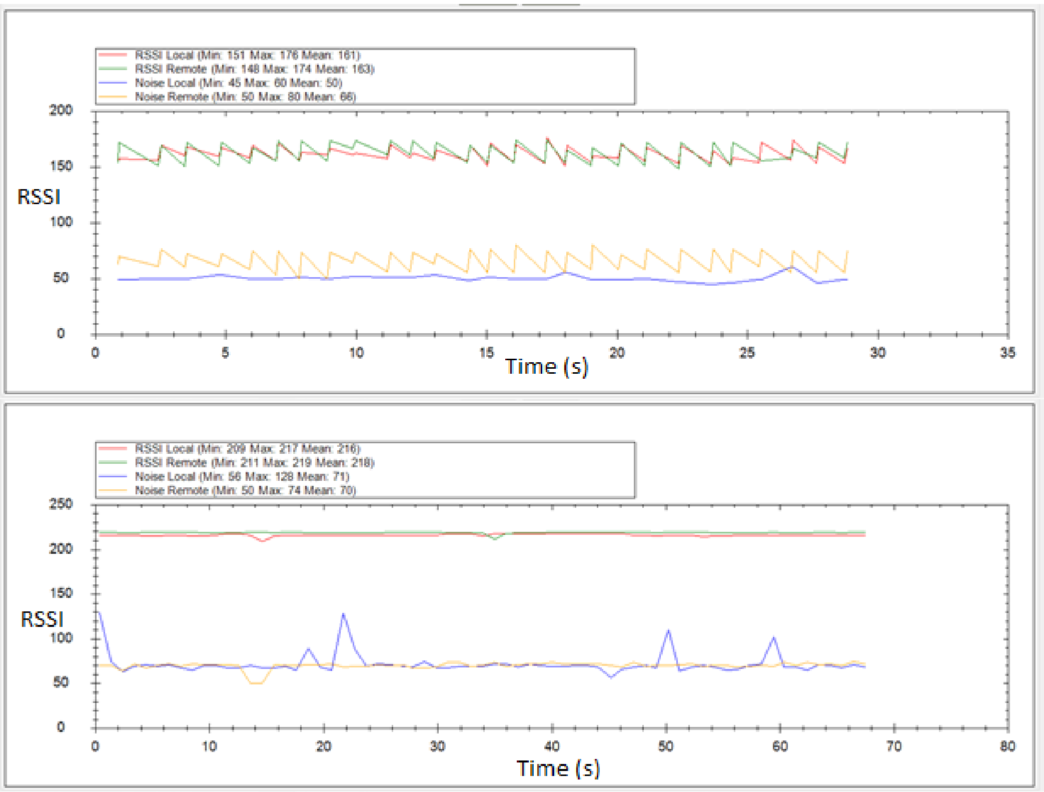


Figure 6.3: RSSI and Noise Vs. Time for local and remote nodes

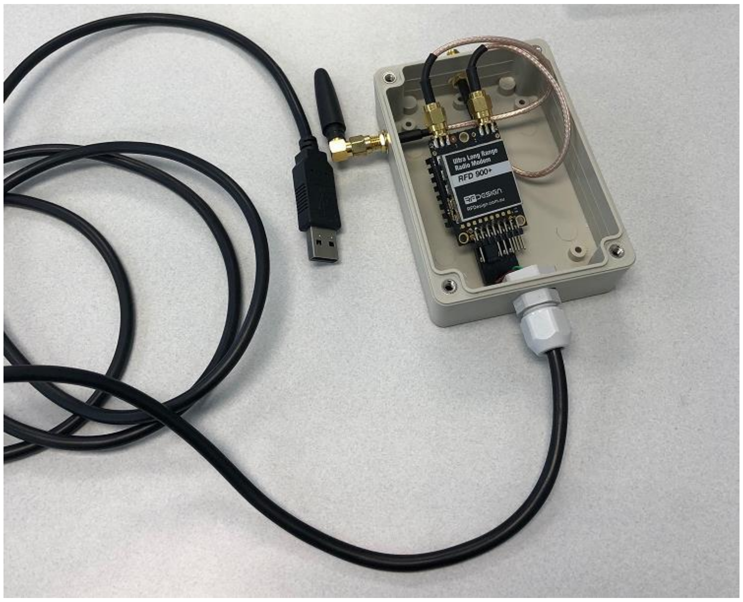


Figure 6.4: RFD900+ Radio Modem as BS

Table 6.1: RFD900+ configurable parameters and their meaning

Parameter	Description	Default	Max	Min
Format	EEPROM Version	---	---	---
Serial Speed	In one byte form	57	115	2
Air Speed	Data rate in one byte	64	250	2
Net ID	Network ID	25	499	0
Tx Power	In dBm	20	30	0
ECC	Error Correcting Code	0	1	0
Mavlink	Mavlink Framing & Reporting	0	1	0
Op Resend	Opportunic Resend	0	1	0
Min Freq	In KHz	915,000	927,000	902,000
Max Freq	In KHz	9228,000	928,000	903,000
Num Channel	Frequency hopping channels	20	50	5
Duty Cycle	Percentage of time to transmit	100	100	10
LBT Rssi	Listen before talk	0	1	0
Manchester	Manchester encoding	0	1	0
RTS CTS	Ready / Clear to send	0	1	0
Node ID	Unique ID for each node	2	29	0
Node Dest	Remote ID to communicate with	65535	29	0
Sync Any	Broadcast feature	0	1	0
Node Count	Total number of nodes	2	30	2

6.3 Evaluation and Results

We focus on showing results for point-to-point and multipoint communications in outdoor experiments since our motive behind this work is to analyze the communications among a fleet of ASVs.

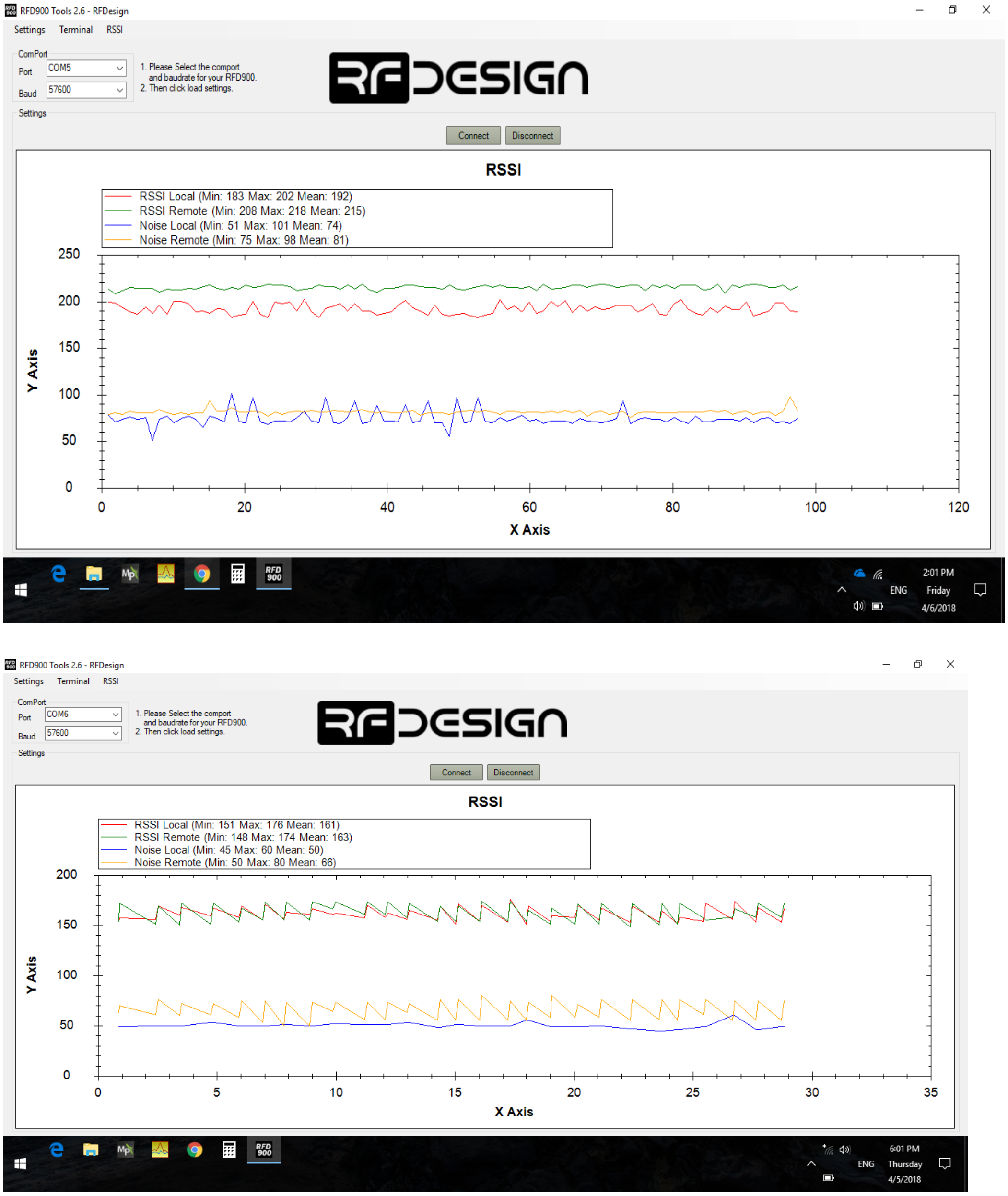
Figure 6.5: Preparation and setting up for outdoor Experiments

6.3.1 Point-to-Point

We were able to achieve robust and reliable communications between the two Jetyaks with data rate up to 250 kps with no issues. Below we show the optimal configuration that we used when running experiments.

```
[0] S0: FORMAT=27                         [1] S0: FORMAT=27
[0] S1: SERIAL_SPEED=57                   [1] S1: SERIAL_SPEED=57
[0] S2: AIR_SPEED=250                     [1] S2: AIR_SPEED=250
[0] S3: NETID=36                          [1] S3: NETID=36
[0] S4: TXPOWER=30                        [1] S4: TXPOWER=30
[0] S5: ECC=0                             [1] S5: ECC=0
[0] S6: MAVLINK=1                         [1] S6: MAVLINK=1
[0] S7: OPPRESEND=0                       [1] S7: OPPRESEND=0
[0] S8: MIN_FREQ=915000                   [1] S8: MIN_FREQ=915000
[0] S9: MAX_FREQ=928000                   [1] S9: MAX_FREQ=928000
[0] S10: NUM_CHANNELS=50                  [1] S10: NUM_CHANNELS=50
[0] S11: DUTY_CYCLE=50                    [1] S11: DUTY_CYCLE=100
[0] S12: LBT_RSSI=0                       [1] S12: LBT_RSSI=0
[0] S13: MANCHESTER=0                     [1] S13: MANCHESTER=0
[0] S14: RTSCTS=0                         [1] S14: RTSCTS=0
[0] S15: NODEID=0                         [1] S15: NODEID=1
[0] S16: NODEDESTINATION=1                [1] S16: NODEDESTINATION=0
[0] S17: SYNCANY=0                        [1] S17: SYNCANY=0
[0] S18: NODECOUNT=2                      [1] S18: NODECOUNT=2
```

In figure 6.6, we show RSSI and noise for both remote and local nodes that correspond to the same experiment. It is worth mentioning that we were able to achieve over 15 miles of robust communication on the river between base station and one surfing Jetyak.


RFD900 Tools 2.6 - RFDesign

ComPort
Port: COM5
Baud: 57600

1. Please Select the comport and baudrate for your RFD900.
2. Then click load settings.

RSSI Local (Min: 183 Max: 202 Mean: 192)
RSSI Remote (Min: 208 Max: 218 Mean: 215)
Noise Local (Min: 51 Max: 101 Mean: 74)
Noise Remote (Min: 75 Max: 98 Mean: 81)

RFD900 Tools 2.6 - RFDesign

ComPort
Port: COM6
Baud: 57600

1. Please Select the comport and baudrate for your RFD900.
2. Then click load settings.

RSSI Local (Min: 151 Max: 176 Mean: 161)
RSSI Remote (Min: 148 Max: 174 Mean: 163)
Noise Local (Min: 45 Max: 60 Mean: 50)
Noise Remote (Min: 50 Max: 80 Mean: 66)

Figure 6.6 : RSSI and Noise results values in Point-to-Point scenarios

6.3.2 Multipoint (3-way)

We setup one base-station and two remote nodes (Jetyaks) to evaluate a three-way communication. Upon adding another Jetyak to serve as an extra remote node, we notice that communications get sluggish and drop pretty quickly (within few meters) when using same exact configurations introduced in the previous point-to-point scenarios. Several configurations were tested to find the optimal values where base station was setup to transmit by broadcast sometimes and transmit to a particular node ID some others. At the later case, the third node was setup to be enabled to SYNC any node or communications in the air. A working configuration sample is shown below, where all nodes were setup to broadcast at the same time. Although this configuration works fine nevertheless it showed high sensitivity to distance and environmental noise. Fig 6.7 shows RSSI and noise value for the setup where all nodes were broadcasting at same time. It is obvious that nodes suffered from noise created by neighboring nodes when they transmit at same time

```
[0] S0: FORMAT=27              [2] S0: FORMAT=27              [1] S0: FORMAT=27
[0] S1: SERIAL_SPEED=57        [2] S1: SERIAL_SPEED=57        [1] S1: SERIAL_SPEED=57
[0] S2: AIR_SPEED=64           [2] S2: AIR_SPEED=64           [1] S2: AIR_SPEED=64
[0] S3: NETID=60               [2] S3: NETID=60               [1] S3: NETID=60
[0] S4: TXPOWER=30             [2] S4: TXPOWER=30             [1] S4: TXPOWER
[0] S5: ECC=0                  [2] S5: ECC=0                  [1] S5: ECC=0
[0] S6: MAVLINK=1              [2] S6: MAVLINK=1              [1] S6: MAVLINK=1
[0] S7: OPPRESEND=0            [2] S7: OPPRESEND=0            [1] S7: OPPRESEND=0
[0] S8: MIN_FREQ=915000        [2] S8: MIN_FREQ=915000        [1] S8: MIN_FREQ=915000
[0] S9: MAX_FREQ=928000        [2] S9: MAX_FREQ=928000        [1] S9: MAX_FREQ=928000
[0] S10: NUM_CHANN=50          [2] S10: NUM_CHANN=50          [1] S10: NUM_CHANN=50
[0] S11: DUTY_CYCLE=20         [2] S11: DUTY_CYCLE=40         [1] S11: DUTY_CYCLE=40
[0] S12: LBT_RSSI=0            [2] S12: LBT_RSSI=0            [1] S12: LBT_RSSI=0
[0] S13: MANCHESTER=0          [2] S13: MANCHESTER=0          [1] S13: MANCHESTER=0
[0] S14: RTSCTS=1              [2] S14: RTSCTS=1              [1] S14: RTSCTS
[0] S15: NODEID=0              [2] S15: NODEID=2              [1] S15: NODEID=1
[0] S16:                       [2] S16:                       [1] S16:
NODEDESTINATION=65535          NODEDESTINATION=65535          NODEDESTINATION=65535
[0] S17: SYNCANY=1             [2] S17: SYNCANY=1             [1] S17: SYNCANY=1
[0] S18: NODECOUNT=3           [2] S18: NODECOUNT=3           [1] S18: NODECOUNT=3
```

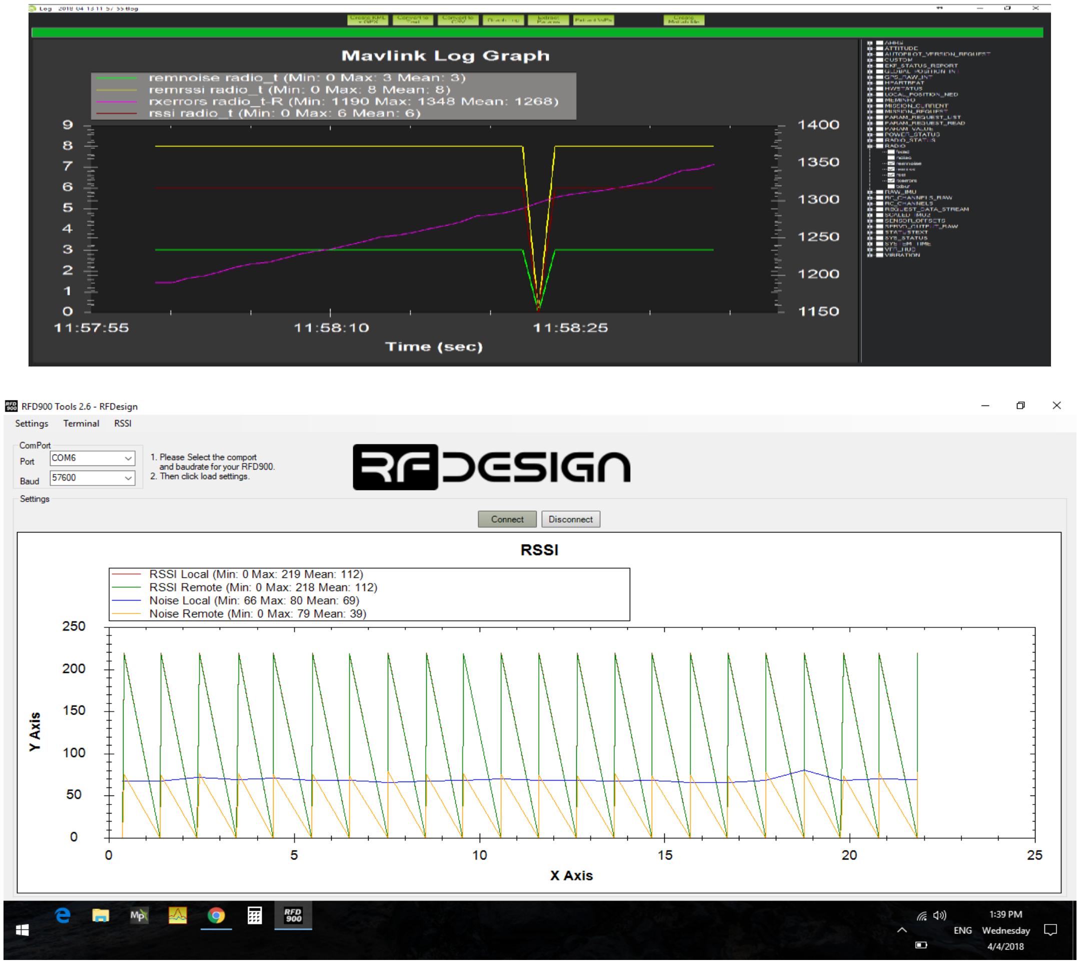

Mavlink Log Graph
remnoise radio_t (Min: 0 Max: 3 Mean: 3)
remrssi radio_t (Min: 0 Max: 8 Mean: 8)
rxerrors radio_t-R (Min: 1190 Max: 1348 Mean: 1268)
rssi radio_t (Min: 0 Max: 6 Mean: 6)
9 8 7 6 5 4 3 2 1 0
1400 1350 1300 1250 1200 1150
11:57:55 11:58:10 11:58:25
Time (sec)
RFD900 Tools 2.6 - RFDesign
Settings Terminal RSSI
ComPort
Port COM6
Baud 57600
1. Please Select the comport and baudrate for your RFD900.
2. Then click load settings.
Settings
RFDESIGN
Connect
Disconnect
RSSI
RSSI Local (Min: 0 Max: 219 Mean: 112)
RSSI Remote (Min: 0 Max: 218 Mean: 112)
Noise Local (Min: 66 Max: 80 Mean: 69)
Noise Remote (Min: 0 Max: 79 Mean: 39)
250 200 150 100 50 0
Y Axis
0 5 10 15 20 25
X Axis
1:39 PM
ENG Wednesday 4/4/2018

Figure 6.7: RSSI and Noise values for local and remote nodes in Multipoint scenario obtained from mission planner (Top) and RFD-Design SW (Bottom)

6.4 Conclusion and Discussion

In this chapter, we discussed and showed the possibility to use the ISM band 900MHz for multipoint communications. Although, the data rate had to be dropped significantly (more than half), to withstand the noise created from environment and neighboring nodes, nevertheless, some tuning is possible to enhance the quality of the communications. The key observation from all experiments tat were conducted is that one needs to decide the size of the communication area, number of communicating nodes, data exchange rate, and the tolerated error. We also were able to achieve a better result in multipoint scenarios in term of data error rate when adjusting the NODE_DESTINATION and SYNC_ANY parameters. However, the exchanged data rate was also dropped which means fewer data were able to be exchanged. In short, using the 900MHz to for monitoring nodes in an open area is cheap and possible solution in LOS environments.

REFERENCES

[1] N. Lyamin, A. Vinel, M. Jonson, and J. Loo, *Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks*, IEEE Communication Letters, VOL. 18, NO. 1, 2014.

[2] R. Raw, M. Kumar, and N. Singh, *Security Challenges, Issues and Their Solutions for VANET*, Vol.5, pp95-105, IJNSA 2013.

[3] A. Hamieh, J. Othman and L. Mokdad, *Detection of Radio Interference Attacks in VANET*, IEEE, 2009.

[4] S. Tengstrand, K. Fors, P. Stenumgaard, and K. Wiklundh, *Jamming and interference vulnerability of IEEE 802.11p*, EMC Europe 2014.

[5] H. Minh, A. Benslimane and A. Rachedi, *Jamming detection on 802.11p under multi-channel operation in vehicular networks*, Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on, Abu Dhabi, 2015, pp. 764-770.

[6] Y. Qian, K. Lu, and N. Moayeri, *A Secure VANET MAC Protocol for DSRC Applications*, IEEE Globecom, 2008.

[7] U.S. Department of Transportation, IntelligentTransportation Systems (ITS) Home, http://www.its.dot.gov/index.htm

[8] U.S. Department of Transportation, IntelligentTransportation Systems (ITS), *IEEE1609 Family of Standards for Wireless Access in Vehicular Environment (WAVE*), http://www.standards.its.dot.gov/Factsheets/Factsheet/80

[9] U.S. Department of Transportation, IntelligentTransportation Systems (ITS), DSRC: *The Future of Safer Driving*, http://www.its.dot.gov/factsheets/dsrc factsheet.htm

[10] National Highway Traffic Safety Administration, *Laws & Regulations, Vehicles*, http://www.nhtsa.gov

[11] Y. Li,An *Overview of the DSRC/WAVE Technology*, International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. Springer Berlin Heidelberg, 2010, pp. 544-558.

[12] SAE Standard J2735 SAE International DSRC Committee, *Dedicated Short Range Communications (DSRC) Message Set Dictionary*, SAE International, 2016.

[13] W. Xu, W. Trappe, Y. Zhang, and T. Wood, *The feasibility of Launching and Detecting Jamming Attacks in Wireless Networks*, MobiHoc, 2005.

[14] L. Humeng, Y. Xuemei, A. Li, and W. Yuan, *Distributed Beacon Frequency Control Algorithm for VANETs (DBFC)*, ISDEA 2012

[15] A. Abdelgader, and W. Lenan, *The physical Layer of the IEEE802.11p WAVE Communications Standard: The Specifications and Challenges*, Vol II, WCECS 2014.

[16] F. Nyongesa, K. Djouani, T. Olwal and Y. Hamam, *Doppler Shift Compensation Schemes in VANETs*, Mobile Information Systems (MIS), vol. 2015, Article ID 438159, 11 pages, 2015.

[17] Z. Rawashdeh, and S. Mahmud, *Communications in Vehicular Ad Hoc Networks*, Mobile Ad-Hoc Networks: Applications, ISBN: 978-953-307- 416-0, InTech 2011.

[18] R. Reinders, M. Eenennaam, G. Karagiannis, and G. Heijenk, *Contention Window Analysis for Beaconing in VANETs*, 7th IEEE Int'l Wireless Communications and Mobile Computing conference, IWCMC 2011, Turkey, pp. 1481-1487.

[19] W. Alasmary, and W. Zhuang, *Mobility impact in IEEE 802.11p infrastructureless vehicular networks, Ad Hoc Netw*. (2010), doi:10.1016/j.adhoc.2010.06.006

[20] NHTSA's National Center for Statistics and Analysis, Traffic Safety Facts, Research Note, U.S. Department of Transportation. National Highway Traffic Safety Administration, 2010.

[21] F. Nadeem, S. Chessa, E. Leitgeb, and S. Zaman, *The Effects of Weather on the Life Time of Wireless Sensor Networks Using FSO/RF Communication*, Radio Engineering, Vol. 19, No. 2, 2010.

[22] C. Boano, N. Tsiftes, T. Voigt, J. Brown, U. Roedig *The impact of temperature on outdoor industrial sensornet applications* IEEE Transactions on Industrial Informatics, 6 (August (3)) (2010), pp. 451–459

[23] J. Bonvoisin, A. Lelah, F. Mathieux, and D. Brissaud, *An environmental assessment method for wireless sensor networks* Journal of Cleaner Production, 33 (September) (2012), pp. 145–154.

[24] F. Martinez, C. Toh, J. Cano, C. Calafate, and P. Manzoni, *A survey and comparative study for vehicular ad hoc networks (VANETs)*, Wiley InterScience, Wirel. Commun. Mob. Comput., DOI: 10.1002/wcm, 2009.

[25] N. Mittal, and S. Choudhary, *Comparative Study of Simulators for Vehicular Ad-hoc Networks (VANETs)*, International IJETAE, Volume 4, Issue 4, 2014.

[26] A Dhamgaye, and N Chavhan, "*Survey on Security Challenges in VANET*", Vol.2, pp88-96, IJCSN 2013.

[27] R Kumar, and M Dave, “*A Comparative Study of Various Routing Protocols in VANET*”, Vol.8, pp643-648, IJCSI 2011.

[28] J Nzouonta, N Rajgure, G Wang, and C Borcea, “*VANET Routing on City Roads Using Real-Time Vehicular Traffic Information*”, Vol. 58, pp3609-3626, IEEE, September 2009

[29] R. Dass, R. Sangwan, and I. Girdhar, “*Vehicular Ad Hoc Networks*”, IJATCSE, Vol.1, October 2012.

[30] M Abdellatif, “ *A Brief Summary on the Main Aspects and Challenges of Vehicular Ad-Hoc Networks (VANETs)*”, INESC Porto, 2010.

[31] G. Samara, W. Al-Salihi, and R. Sures,”*Security Analysis of Vehicular Ad Hoc Networks*”, 2nd NETAPPS, 2010.

[32] H. Hartenstein, and K. Laberteaux, “*VANET: Vehicle Applications and Inter-Networking Technologies*”, John Wiley & Sons Ltd., 2010

[33] Cooperative Vehicle-Infrastructure Systems,”*FleetNet*”, http://www.cvisproject.org/en/links/fleetnet.htm, 2014

[34] A. Festag, G. Noecker, M. Strassberger, A. Lübke, B. Bochow, M. Torrent-Moreno, S. Schnaufer, R. Eigner, C. Catrinescu, and J. Kunisch,”*NoW – Network on Wheels’: Project Objectives, Technology and Achievements*”, International Workshop on Intelligent Transportation (WIT), 2008.

[35] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “J*amming Sensor Networks: Attack and Defense Strategies*”, IEEE 2006.

[36] H. Mustafa, X. Zhang, Z. Liu, W. Xu, and A. Perrig, “*Jamming-Resilient Multipath Routing*”, IEEE, Vol. 9, 2012.

[37] K. Siddhabathula, “*Fast jamming detection in wireless sensor networks*,” University of Texas, 2011.

[38] Y. Zhu, X. Li, and B. Li, “*Optimal Adaptive Anti jamming in Wireless Sensor Networks*”, International Journal of Distributed Sensor Networks (IJDSN2012), Volume 2012.

[39] Federal Communications Commission, Enforcement Bureau, ”*GPS, Wi-Fi, and Cell Phone Jammers*”, http://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf.

[40] I. Sumra, H. Hasbullah, J. Lail, and M. Rehman, “*Trust and trusted computing in vanet*”, Computer Science Journal, 2011.

[41] H. Hasbullah, I. Soomro, and J. Manan, “*Denial of Service (DOS) Attack and Its Possible Solutions in VANET*”, World Academy of Science, Engineering and Technology, 2010

[42] S. Babar, N. Prasad, and R. Prasad, “*Jamming Attack: Behavioral Modeling and Analysis*”, IEEE, 2013.

[43] I. Azogu, M. Ferreira, J. Larcom, and H. Liu, “*A New Anti-Jamming Strategy for VANET*”, Globecom 2013 Workshop, IEEE, 2013.

[44] S. Bhoi, and P. Khilar, “*A Secure Routing Protocol for Vehicular Ad Hoc Network to Provide ITS Services*”,International conference on Communication and Signal Processing 2013, IEEE, 2013.

[45] J. Sarker, and H. Mouftah, “*Mitigating the effect of jamming signals in wireless ad hoc and sensor networks*”, IET Communications, 2012.

[46] A. Nguyen, L. Mokdad, and J. Ben-Othman, “Solution of Detecting Jamming Attacks in Vehicle Ad Hoc NETworks”, ACM, 2013.

[47] Y. Kim, P. Tague, H. Lee, and H. Kim, “*Carving Secure Wi-Fi Zones with Defensive Jamming*”, ACM, 2012.

[48] Z. Lu, W. Wang, and C. Wang, “M*odeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications*”, IEEE transaction on Mobile Computing, 2014.

[49] I. Aziz, and S. Yadav, “*Data Encapsulation To Prevent Jamming Attacks In Wireless Networks*”, IJCTA, 2013.

[50] A. Proano, and L. Lazos, “Packet-*Hiding Methods for Preventing Selective Jamming Attacks*”, IEEE ICC, 2010.

[51] G. Rash, “*GPS Jamming in A Laboratory Environment*”, http://fas.org/spp/military/program/nav/labjam.pdf, NAWCWPNS, 2014.

[52] Y. Zhang, and M. Amin, “*Anti-Jamming GPS Receiver With Reduced Phase Distortions*”, IEEE SIGNAL PROCESSING LETTERS, 2012.

[53] T. Kaur, and S. Sharma, “*Mitigating the Impact of Jamming Attack by Using Antenna Patterns in MANET*”, IJCSIT, 2012.

[54] S. Jasim, “*Jamming Attacks Impact on the Performance of Mobile Ad-Hoc Network and Improvement Using MANET Routing Protocols*”, IJETA, 2013.

[55] J. Ajana, J. Helen, “*Mitigating Inside Jammers in Manet Using Localized Detection Scheme*”, IJESI, 2013.

[56] J. Xiong, and K. Jamieson, “*SecureArray: Improving WiFi Security with Fine-Grained Physical-Layer Information*”, ACM, 2013.

[57] H. Pareek, and V. Shrivastva, “*Denial of Service Attacks Implementation and Detection Approach for MANET*”, International Journal of Advanced Research in Computer and Communication Engineering, 2014.

[58] S. Waharte, N. Trigoni, and S. Julier, “Coordinated search with a swarm of UAVs,” in IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 2009.

[59] M. Asadpour, B. V. den Bergh, D. Giustiniano, K. A. Hummel, S. Pollin, and B. Plattner, “Micro aerial vehicle networks: an experimental analysis of challenges and opportunities,” IEEE Communications Magazine, vol. 52, no. 7, pp. 141–149, July 2014.

[60] S. Hayat, E. Yanmaz, and C. Bettstetter, “Experimental analysis of multipoint-to-point UAV communications with IEEE 802.11n and 802.11ac,” in IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Aug 2015, pp. 1991–1996.

[61] S. Morgenthaler, T. Braun, Z. Zhao, T. Staub, and M. Anwander, “UAVNet: A mobile wireless mesh network using unmanned aerial vehicles,” in IEEE Globecom Workshops, Dec 2012, pp. 1603–1608.

[62] P. K. Penumarthi, A. Quattrini Li, J. Banfi, N. Basilico, F. Amigoni, I. Rekleitis, J. M. O’Kane, and S. Nelakuditi, “Multirobot exploration for building communication maps with prior from communication models,” in International Symposium on Multi-Robot and Multi-Agent Systems, Los Angeles, CA, USA, Dec. 2017.

[63] J. Banfi, A. Quattrini Li, N. Basilico, I. Rekleitis, and F. Amigoni, “Asynchronous multirobot exploration under recurrent connectivity constraints,” in IEEE International Conference on Robotics and Automation (ICRA), Stockholm, Sweden, May 2016, pp. 5491–5498.

[64] C. Team, “Volkswagen To Make Cars That Can Communicate With Each Other”, https://auto.ndtv.com/news/volkswagen-to-make-cars-that-can-communicate-with-each-other-1718555, Jun 29, 2017 05:55 PM, Last accessed Jun 13, 2018.

[65] Google selfdriving-car project, “https://waymo.com/”, last accessed on Jun 13, 2018.

[66] B. Howard, “Cadillac Promises Self-Driving Cars by 2015”, http://www.extremetech.com/extreme/126841-cadillac-promises-self-driving-cars-by-2015, April 23, 2012, Last accessed Jun 13, 2018.

APPENDIX A

Evaluation Tool- Toward a Realistic VANET Simulator

In [24-25] authors have surveyed different network simulators that support building and simulating VANET. They evaluated at least 10 different simulators in terms of protocols and services in a variety of conditions (number of nodes, traffic, congestion, SNR, fading, path loss, etc). Based on the comparative study [24-25], we choose to use National Chiao Tung University Network Simulator (NCTUns) as an evaluation tool for this work. The simulator was originally developed as a network simulator with unique capabilities. Several releases have been introduced to accommodate new technology as they evolved. In this work we use the sixth release of NCTUns 6.0 that incorporate traffic simulation (e.g., road network construction and vehicle mobility models).

A. Modules

Several modules are supported by NCTUns that makes it flexible as an evaluation tool. NCTUns also support the integration of 802.11p/WAVE standards to provide a realistic evaluation results. Nevertheless, NCTUns also supports creating, modifying or adding modules to the workspace.

B. Nodes Parameters & mobility

When simulating VANET, we need to consider the different nodes (RSUs, OBUs). Each node need to be configured differently since different standards are available for different nodes. For instance, only RSUs can advertise on the CCH and announce available services on different SCHs. Also, RSUs can't have any mobility models since they are infrastructural towers. On the other hand, NCTUns two different mobility models to support the mobility of vehicles nodes (agent-controlled \& Module-controlled). Additionally, NCTUns give free access through its GUI to adjust different parameters for each node (signal power, receiving sensitivity, fading models, obstacles, speed, direction etc.) which is supported by NCTUns.

C. Channel Model

Simulating using NCTUns enables user to choose from two kinds of channel models: Theoretical and Empirical. Within theoretical channel model NCTUns supports three theoretical path-loss models (free-space, two-ray ground, and free space and shadowing). Additionally, Rayleigh, Ricean and no-fading are also supported by the simulator to choose from as fading mode.