UNIFIED DISTRIBUTION OF PSEUDONYMS IN HYBRID EPHEMERAL VEHICULAR NETWORKS

A Dissertation
Presented to
The Academic Faculty

by

Joseph T. Benin

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

Georgia Institute of Technology
December 2012

UNIFIED DISTRIBUTION OF PSEUDONYMS IN HYBRID EPHEMERAL VEHICULAR NETWORKS

Approved by:

Dr. Henry Owen, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. John Copeland
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. George Riley
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Raheem Beyah
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Mustaque Ahamad
School of Computer Science
Georgia Institute of Technology

Date Approved: 11/7/2012

To Good Samaritans, who help others in need, regardless of race, sex, or creed.

ACKNOWLEDGEMENTS

Any work-intensive accomplishment is the result of the support, guidance, and love of all those who are involved, both directly and indirectly, in that endeavor. To this end, there are not enough pages for me to inscribe all the names of those who deserve mention for positively molding me but I must recognize some. First I wish to acknowledge the Supreme Being, infinitely perfect, Who made all things, and keeps them in existence. My gratitude for my existence, abilities, and sustainment has no bounds.

Next I wish to acknowledge my family starting with my wife, Rachel, who has supported me to the best of her ability in the midst of tremendous tragedy and suffering. I wish to thank my parents who have always encouraged my development and education, even at their own personal sacrifice. And I thank my children, Rebecca, Joey, and Jeanette, for their inspiration, joy, and affection. I also wish to thank my mother- and father-in-law for their understanding and counsel during the dark days. I wish to acknowledge my sisters, Jennifer and Christina, my sister-in-law, Elizabeth, and my grandmother-in-law, Mrs. Lena Waller, for their words of encouragement at the right times. Special gratitude is extended to Mrs. Johanna Haggerty ("Mutti") and her son, Dr. Paul Haggerty, who is and has been a brother to me.

In terms of this doctoral journey, for his professional academic guidance and personal care and concern I express my deepest appreciation for Dr. Henry Owen III, my primary advisor and a wonderful man. I also wish to acknowledge all those who served on my committee: Dr. Copeland, Dr. Riley, Dr. Beyah, and Dr. Ahamad. Thank you for your participation in this process and feedback. I also wish to thank the other members of the Network Security Architecture and Communications Systems Center labs, most especially Dr. Nowatkowski, Dr. Fairbanks, Dr. Zhou, and Mr. Khan, for the invigorating technical discussions. I offer a special thanks to all the faculty and staff of the Georgia Institute of Technology who assisted me in pursuing graduate education, especially Dr. Hertling, Ms. Mycko (the finest graduate advisor), Ms. Treppier, Dr. Dorsey, Dr. Goodman, and Dr. Havick.

I express my sincere gratitude to the many friends I have been blessed with in life, especially Rev. Vaccaro, Mr. Soliven, Rev. Ketter, Mr. Norte, Mrs. Wong, Mr. & Mrs. Bauer, LCDR & Mrs. Chien, LCDR Edwards, CDR & Mrs. Godfrey, Mrs. Lawless, LT

Maca, Miss Naranjo, Mr. O'Brien, and Mr. & Mrs. Shaw. These and so many have been there for me from my childhood, Seton High School and Academy days, time in Seattle, time in Connecticut, and time in Atlanta providing the encouragement needed to push forward with life's pursuits, academic and otherwise.

I also wish to express my gratitude to the United States Coast Guard and the faculty and staff of the Coast Guard Academy who facilitated my education in the ways of Electrical Engineering, Leadership, and, in many ways, Life. I have been blessed with many great mentors, chief among them Dr. Keith Gross (RIP). To him and the other fine members of the Coast Guard and Academy, including CAPT Dillon (RIP), CAPT Hartnett, CDR Bruckner (ret), CDR Oatman, CDR Staier, CDR Pickles, LCDR Seals, ETCM O'Connell, Dr. Ringel, Dr. Allen and Mrs. Zakutansky, I express my gratitude. I also thank the cadets who motivated me to want to pursue being a member of the PCTS and this degree.

Finally, from the bottom of my heart, I thank all those Good Samaritans who without I could not have completed this dissertation. Those in France (especially Mrs. Sands and Dr. Binet), those in Atlanta (especially Mrs. Abraham, Mrs. Child, Mrs. Davidson, Mr. Gnanapragasam, Miss Goldman, Miss Kroll, Mr. & Mrs. Maroney, The Miller Family, Mr. Mirabile, Mr. Murphy, Mr. & Mrs. Rue, Dr. Satre, Mrs. Spangler, Mr. & Mrs. Townsend, Mr. & Mrs. Troutman, Mr. & Mrs. Uebelacker, Mr. & Mrs. Wuerslin, and the St. Jude Parish family, especially my CRHP brothers and sisters), and all those who prayed for and supported me but are not named.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

AIFS	Arbitration InterFrame Space (used by the QoS facility of 802.11)
AC	Access Category
ASTM	Formally the American Society for Testing and Measurement and now known as ASTM International
CA	Certificate Authority
CACS	Comprehensive Automobile Traffic Control System
CCH	Control Channel (i.e. 178)
CRL	Certificate Revocation List
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
DSRC	Dedicated Short Range Communication
ECDSA	Elliptical Curve Digital Signature Algorithm
EDCA	Enhanced Distributed Channel Access
ERGS	Electronic Route-Guidance System
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
IEEE	Institute for Electrical and Electronics Engineers
IFS	InterFrame Space (time interval between 802.11 frames)
ITS	Intelligent Transportation System
ns-3	Network Simulator (3rd and current instantiation)
OBU	On Board Unit
OFDM	Orthogonal Frequency-Division Multiplexing
PKI	Public Key Infrastructure
PN	Pseudonym
PNDP	Pseudonym Distribution Protocol
QoS	Quality of Service
RA	Registration Authority
RFC	Request for Proposal
RSU	Road Side Unit
SCH	Service Channel (i.e. 172, 174, 176, 180, 182, 184)

SRMP	Short Range Message Protocol
TCP	Transport Control Protocol
TPD	Tamper Proof Device
UDP	Universal Datagram Protocol
V2I	Vehicle to Infrastructure (communications)
V2V	Vehicle to Vehicle (communications)
VANET	Vehicle Ad Hoc Network (also known as a vehicular network)
VPKI	Vehicular or VANET Public Key Infrastructure
VN	Vehicular Network (also known as VANETs)
WAVE	Wireless Access in Vehicular Environments
WSMP	WAVE Short Message Protocol

SUMMARY

The objective of this research is to devise a unified method for the distribution of pseudonyms in ephemeral hybrid vehicular networks, which are often referred to as vehicular ad hoc networks (VANETs), for the purposes of refill, intra-regional, and inter-regional movement. This work addresses a significant impediment to the use of pseudonyms, which has been almost universally accepted (and is on the verge of being standardized by the Institute for Electrical and Electronic Engineers (IEEE) and the Society for Automotive Engineers (SAE) as the best means to balance attribution and privacy to maximize the value of infrastructure deployment and citizen acceptability (i.e. use). The results include a pseudonym distribution protocol that achieves ease of use while not compromising the security or privacy pseudonyms afford. These results contribute to the solution, in a scalable, adaptive, and bandwidth efficient manner, of one of the remaining impediments to the adoption of VANETs. The new method shows improved performance compared to a baseline pseudonym distribution method that does not take these factors into consideration.

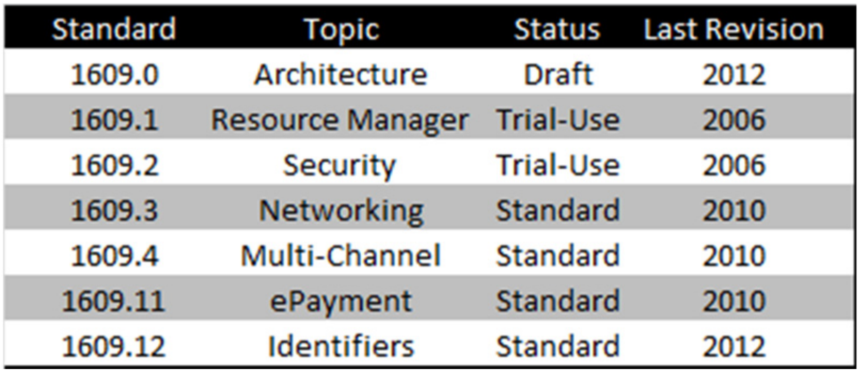
CHAPTER 1

INTRODUCTION

Human beings have sought to transport themselves and goods since the dawning of time. Whether by land, sea, or eventually air and space, transporting physical entities has simply been a part of who we are. At the end of the nineteenth century, moving analog signals over the radio became a reality. Since the early 1970s, the transporting of digital information over a distance has joined the list of things transported in contemporary times. In 1999, wireless networking became standardized with the ratification of the Institute for Electrical and Electronics Engineers (IEEE) 802.11a [1]. Thus it is only natural that these two worlds would converge in the utilization of wireless communications between vehicles.

The idea of cars "talking" to each other is not new. In fact the earliest reference to this activity is believed to be General Motor's "GM Futurama" presented during the 1939 World's Fair in New York City and featured in their movie *To New Horizons*. This was a mere 31 years after the introduction of Henry Ford's Model T and about 40 years after the invention of radio [2]. In 2006 this prediction for 1960 took a huge leap forward with the ratification of the first four members of the family of IEEE 1609 Standards (.1 - .4) for Wireless Access in Vehicular Environments (WAVE). Since then networks involving vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications have been coined VANETs (vehicular ad hoc networks) and are also referred to as "Vehicular Networks" (VNs). (These two terms will be used interchangeably in this dissertation.) Demonstrating a maturation of this effort, the IEEE published ratified full standards to the networking (1609.3), multi-channel (1609.4), and electronic payment (1609.11) members of the 1609 family in 2010 and an additional draft document, IEEE 1609.12, to standardize the identifiers used in VNs [3]. The entire family of IEEE 1609 standards is listed in Table 1 and will be discussed in greater detail below.

Table 1. Summary of IEEE 1609 family of standards.



Standard	Topic	Status	Last Revision
1609.0	Architecture	Draft	2012
1609.1	Resource Manager	Trial-Use	2006
1609.2	Security	Trial-Use	2006
1609.3	Networking	Standard	2010
1609.4	Multi-Channel	Standard	2010
1609.11	ePayment	Standard	2010
1609.12	Identifiers	Standard	2012

The ephemeral nature of vehicles brings to bear an entirely new set of challenges, constraints, and possibilities apart from any other networking paradigm. These will be discussed at length in Section 2 of this dissertation along with the security characteristics required to bring this emerging technology to market and into the vehicles we drive for improved safety (and potentially convenience and infotainment). The work within vehicular networks parallels significant developments in the area of autonomous vehicles. While VNs stand to improve the ability of drivers by augmenting information available to them and possibly automating the response of vehicles to information received, VNs will revolutionize autonomous vehicles much as the TCP/IP protocol stack revolutionized the personal computer. Thanks to this promising research area, the future looks brighter for roadway accident avoidance, driver awareness, and a whole host of VN-enabled autonomous vehicle applications.

1.1 Motivation

The desire for safer roads is virtually universal. Drivers, pedestrians, property owners, tax payers, and the environment all benefit from fewer accidents and congestion. The 2010 traffic safety statistics (the most recent publically available) published by the National Highway Safety Administration of the United States Department of Transportation paint a generally encouraging picture of roadway safety in the United States over the past ten years but still represent a horrific reality of the dangers of driving [4, 5]. In 2010, there were 5,419,000 total accidents including 30,196 fatal crashes, 1,542,000 crashes that resulted in only injuries, and 3,847,000 vehicle accidents that resulted in only property damage. A total of 32,885 people lost their lives in vehicle accidents in 2010 and another 2,239,000 people were injured [5]. These statistics are startling yet they represent the lowest number of traffic fatalities and the second lowest number of injuries in the past 10 years as shown in Figure 1.

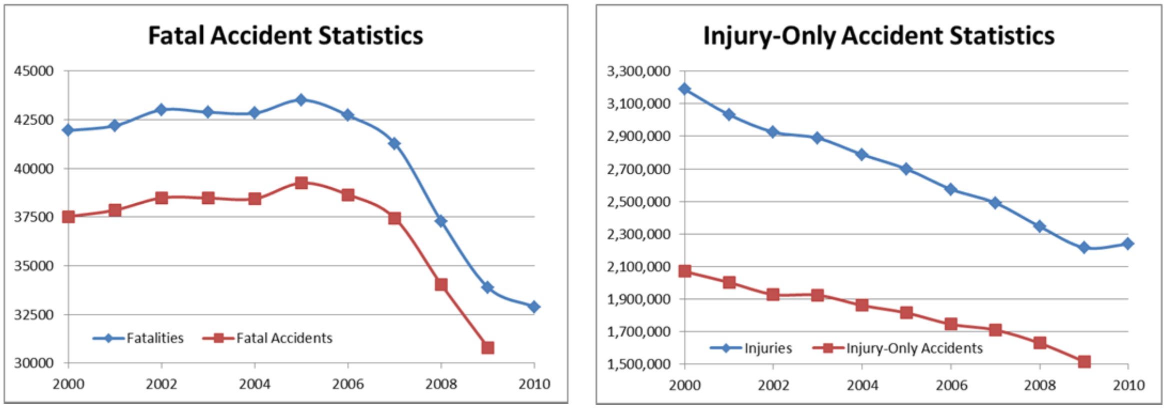


Figure 1. 2000-2010 Vehicle accident statistics in the United States.

One interesting aspect of traffic safety is the comparison of urban and rural driving statistics. In the United States in 2008 (when a study was conducted for this comparison), 15,983 fatalities occurred in urban areas while 20,905 occurred in rural areas. This is more significant given only 23 percent of the population lived in rural areas at that time [6]. Additional research into the geospatial distribution of vehicle accidents and traffic fatalities was conducted by the National Highway Traffic Administration in 2009. They discovered that 44% of traffic fatalities occurred within urban areas that year but if one looked at suburban areas 2.5, 5, 7.5, and 10 miles beyond the urban boundaries, this percentage increased to 63%, 73%, 81%, and 86% respectively [7]. This disproportion and subsequently greater potential for improved safety in rural areas has been recognized by German researchers and caused them to argue that VANETs have an even greater contribution to make for those living and travelling in rural and suburban areas [8].

1.2 Contributions

The primary contributions of this body of work consist in (a) offering a unified framework with novel adjustment for the implementation of a public key infrastructure (PKI) adapted for vehicular use and (b) detailing a comprehensive examination of the many facets that affect pseudonym (PN) distribution and their impact.

This research provides a framework that achieves (beyond the standard security goals of user-message authentication, user privacy, and message integrity) a workable PKI for the VANET environment. Specifically, the presented scheme we developed limits the scope of pseudonyms to recycle the key space, distributes PKI administration across regions to reduce storage and processing requirements on the OBU and Registration Authority (RA), introduces a method for expanding the coverage of VANETs via regions, reduces the size of the certificate revocation list (CRL) needed by a vehicle in order to maintain a dynamic network security posture, and reduces the search space required to authenticate the sender of a message. Ultimately, such a framework provides the proper balance of mobility and privacy.

Within this framework is developed a protocol used to examine the many factors that affect PN distribution. This protocol has been named the PseudoNym Distribution Protocol (PNDP). This results in: (1) a unified protocol that can be used for the transmission of PNs whether for refill (their reloading as the supply expires), usage within a new region under the same CA (intra-regional), or usage within a new region under a different CA (inter-regional); (2) the incorporation of control channel and service channel intervals and the multiple service channels which are uniquely available to networks under the IEEE 1609 standard; (3) the extension of such a protocol across multiple RSUs to provide a more scalable solution to the distribution of PNs problem; and (4) the inclusion of a control mechanism to prevent endless flooding of PNs in these subsequent RSU transmissions.

Finally, various considerations affecting PN distribution and its modeling were investigated. With regards to simulation, proper propagation loss and mobility models were examined to provide more realistic results. With regards to PN distribution considerations, questions of OBU need, data transmission prioritization, pseudonym pre-computation, OBU/RSU cooperation, pseudonym forwarding, and layer two protocol impact were investigated and those results are presented as well.

1.3 Roadmap for Dissertation

This dissertation is organized to guide the reader through an exploration of the topic of vehicular networks which will begin in chapter two. Chapter three then ventures into the world of vehicular public key infrastructures (VPKI) including a discussion of the many features unique to VANETs. An overview of the simulation method used in this thesis is then covered in chapter four with the various scenarios and simulation results presented in chapter five. Chapter six synthesizes the results of the various scenarios and compares this work to other published methods. The thesis concludes with chapter seven featuring recommendations and potential future work.

CHAPTER 2

VEHICULAR NETWORKS

2

2.1 Overview and Historical Development

Vehicular Ad Hoc Networks (VANETs) find their modern beginnings in the development of the intelligent transportation system (ITS) in the late 1970’s and 1980’s [9]. The core goals of VANETs are:

1. increased safety on the road,
2. greater efficiency in the use of the roadways,
3. decreased negative environmental impact from the use of vehicles on the roadways [10, 11].

State- and industry sponsored research specific to VANETs has been ongoing for some time. An Electronic Route-Guidance Systems (ERGS) was proposed in 1970 within the United States by research sponsored by the federal Office of Research and Development, Bureau of Public Roads, but was abandoned due to the high cost of its infrastructure [12]. The Japanese Agency of Industrial Science and Technology of the Ministry of International Trade and Industry sponsored the Comprehensive Automobile Traffic Control System (CACS) from 1973 to 1979 [13]. However it wasn’t until the Federal Communication Commission (FCC) in the United States reserved 75 MHz of bandwidth from 5.850 - 5.925 GHz in October of 1999 for Dedicated Short Range Communication (DSRC) that a new round of global research and development ignited [14]. Figure 2 shows an overview of VANET activities since 1990. The previous US effort sponsored by the Department of Transportation (DOT) is known as IntelliDrive, which, in keeping with the traditional goals of VANETs, strived to make driving "safer, smarter, and greener" [15]. Since 2010, efforts to develop the technology as well as the business case for vehicular networks have only intensified globally. Researchers in China, India, and other countries have joined the international effort to increase roadway safety. All of these efforts have culminated in the United States DOT's Research and Innovative Technology Administration's launching of the Connected Vehicle Safety Pilot Program, whose vision is to "demonstrate the transformative nature and benefits of connected vehicle technologies" and is scheduled to run through the fall of 2013 [16].

The automotive industry remains a significant player and has conducted studies to determine market penetration and how to convert VANETs into a financially solvent proposition. They predict that if all new cars sold were VANET-equipped, a 50% market penetration would be achieved within 7.5 years; if only 50% of new cars sold were so equipped, the same penetration could take 15 years or more [17]. One of the policy issues outside the scope of this research is whether VANETs will be market-driven (like built in navigation systems and rear view cameras) or state-mandated (like seat belts and airbags), which would greatly affect the number of vehicles on the road that are VANET capable.

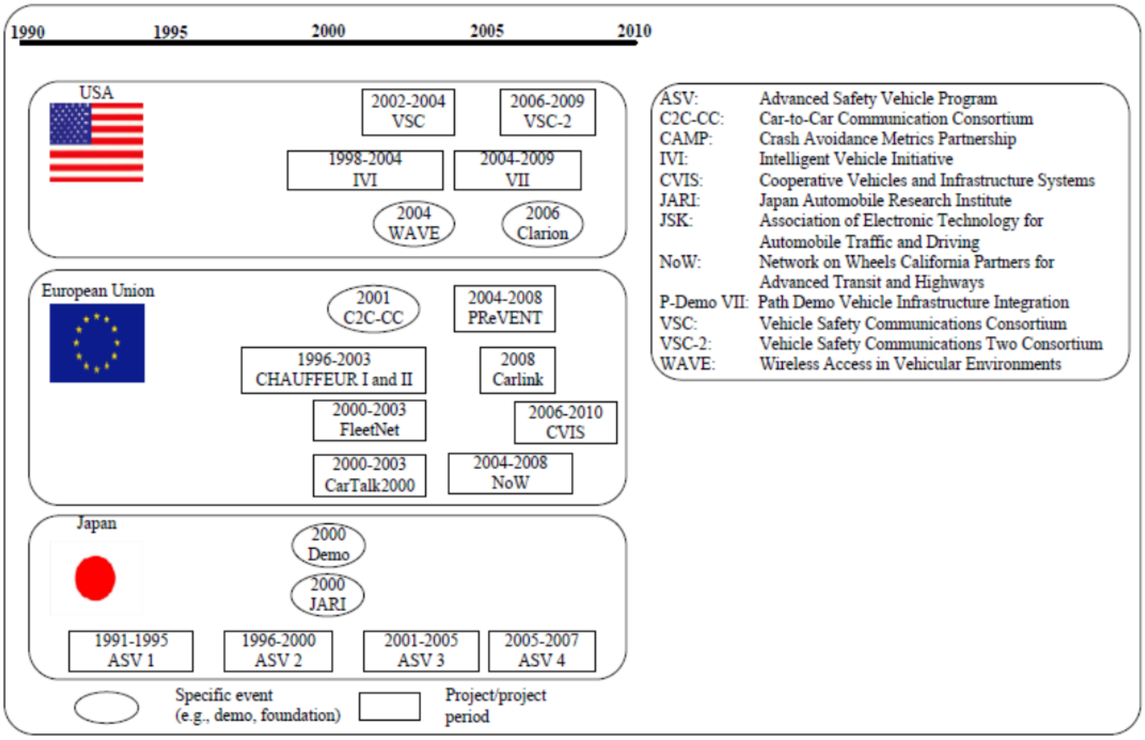

1990
1995
2000
2005
2010
USA
2002-2004 VSC
2006-2009 VSC-2
1998-2004 IVI
2004-2009 VII
2004 WAVE
2006 Clarion
European Union
2001 C2C-CC
2004-2008 PReVENT
1996-2003 CHAUFFEUR I and II
2008 Carlink
2000-2003 FleetNet
2006-2010 CVIS
2000-2003 CarTalk2000
2004-2008 NoW
Japan
2000 Demo
2000 JARI
1991-1995 ASV 1
1996-2000 ASV 2
2001-2005 ASV 3
2005-2007 ASV 4
ASV: Advanced Safety Vehicle Program
C2C-CC: Car-to-Car Communication Consortium
CAMP: Crash Avoidance Metrics Partnership
IVI: Intelligent Vehicle Initiative
CVIS: Cooperative Vehicles and Infrastructure Systems
JARI: Japan Automobile Research Institute
JSK: Association of Electronic Technology for Automobile Traffic and Driving
NoW: Network on Wheels California Partners for Advanced Transit and Highways
P-Demo VII: Path Demo Vehicle Infrastructure Integration
VSC: Vehicle Safety Communications Consortium
VSC-2: Vehicle Safety Communications Two Consortium
WAVE: Wireless Access in Vehicular Environments
Specific event (e.g., demo, foundation)
Project/project period

Figure 2. VANET research in the United States, Europe, and Japan, source: [13].

A VANET consists of a combination of mobile On Board Units (OBUs) which are located on the cars and vehicles themselves (including the potential for bicycles and pedestrians) and geographically fixed Road Side Units (RSUs, which may come in the form of traffic lights, highway lamps, etc) that are interconnected by a backbone network. Thus the OBUs only have direct connectivity to other OBUs and RSUs that are within a given OBU's transmission range (approximately 1000 ft maximum [18], however methods have been offered to decrease the range ("adaptive transmit power" and Distributed Fair Transmit Power Adjustment for Vehicular Ad Hoc Networks (D-FPAV)) and transmission rate ("rate control") in order to increase the number of active participants, such as in [11, 19]). While the RSUs have the ability for "always on" Internet access, the OBUs Internet access cannot be assumed to exist. A series of standards and draft standards govern VANETs while a non-trivial amount of research continues to push its development further to an installed reality.

Figure 3 illustrates the various standards that contribute to defining VANET operation, each of which will now be discussed. Of particular note is the support within VANETs of two distinct upper-layer protocol stacks. On the left is the unique WAVE Short Message Protocol (WSMP) stack that provides for smaller and quicker message exchange and is envisioned for safety-oriented applications. For non-safety related applications, WAVE supports the standard Internet Protocol version 6 (IPv6) network layer with traditional transport layer support as shown on the right of Figure 3.

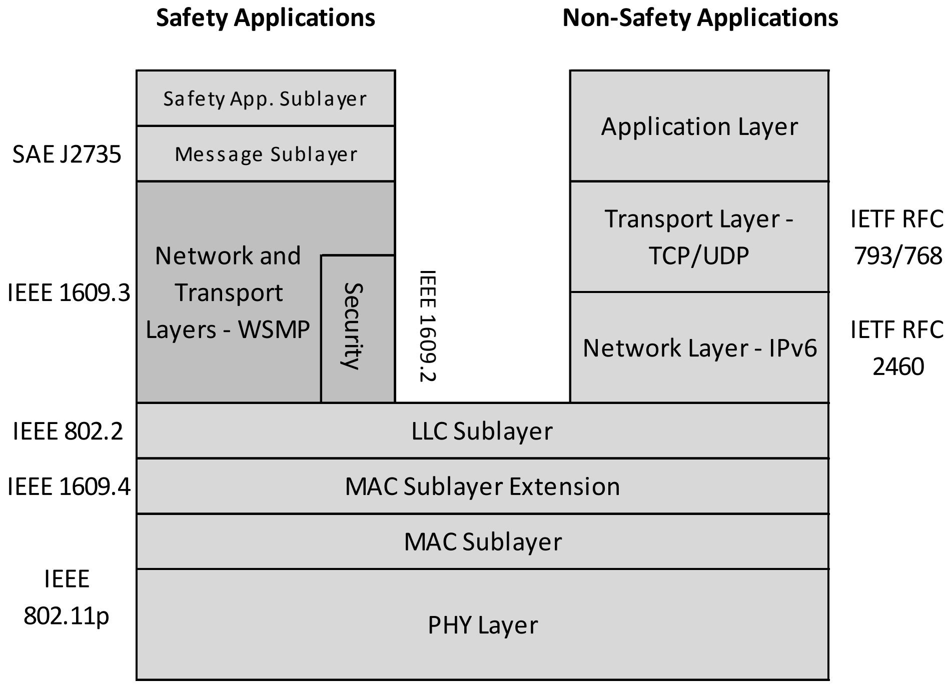
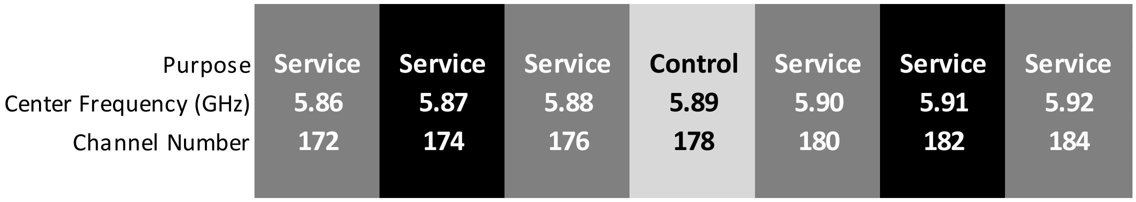


Figure 3. Layered architecture for DSRC communication in the United States (adapted from [13]).

2.1.1 Physical and Data Link Layers (IEEE 802.11p, 1609.4, and 802.2)

The frequency utilization of VANETs was originally outlined in an ASTM International standard for DSRC based upon the general IEEE 802.11 standard. This work was codified as ASTM E2213-03 in 2003 and has since been incorporated into IEEE Standard 802.11p. This standard specifies the use of orthogonal frequency division multiplexing (OFDM) with a nominal bandwidth of 10 MHz (Regulatory Class 17 in the United States and Regulatory Class 14 in Europe); although 5 and 20 MHz channel bandwidths are supportable) [20]. Thus the 75 MHz allocated for DSRC is divided into 7 channels, the first three being service channels (SCH), followed by the control channel (CCH), and three additional service channels, as illustrated in Figure 4. Table 2 lists the maximum achievable data rates for OFDM modulation which are a direct result of the transmit spectral mask (Figure 5), both of which are as specified in 802.11p.



Purpose	Service	Service	Service	Control	Service	Service	Service
Center Frequency (GHz)	5.86	5.87	5.88	5.89	5.90	5.91	5.92
Channel Number	172	174	176	178	180	182	184

Figure 4. WAVE channel configuration.

Table 2. Data rate options in a DSRC 10 MHz OFDM channel ([20] and [13]).

Modulation	Coding Rate (R)	Coded Bit Rate (Mpbs)	Data Rate (Mbps)
BPSK	1/2	6	3
BPSK	3/4	6	4.5
QPSK	1/2	12	6
QPSK	3/4	12	9
16-QAM	1/2	24	12
16-QAM	3/4	24	18
64-QAM	2/3	36	24
64-QAM	3/4	36	27

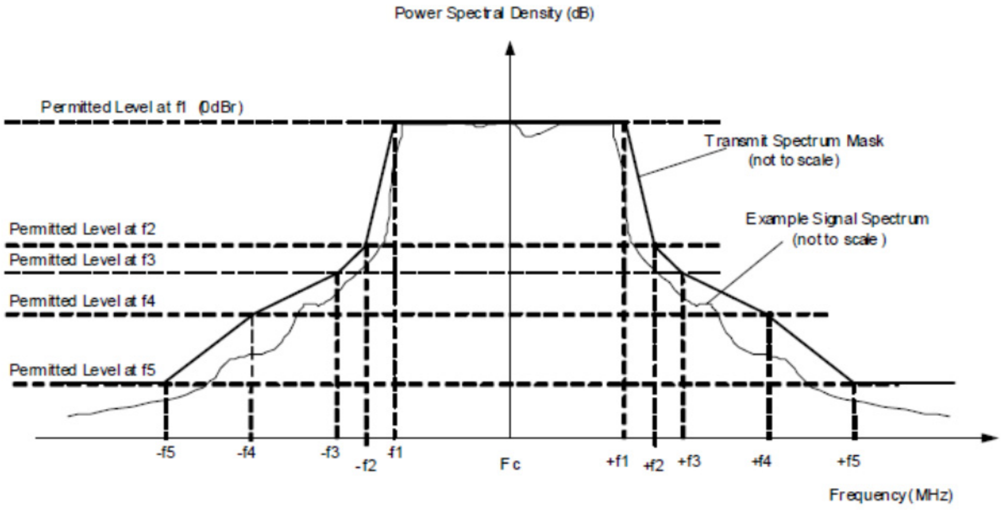


Figure 5. Transmit spectrum mask and application, source: [20].

Of particular note regarding the MAC sublayer is that 802.11p incorporates the carrier sense multiple access/collision avoidance (CSMA/CA) with 802.11's enhanced distributed channel access (EDCA) mechanism. EDCA permits four different access categories (AC) with separate frame queues which constitutes quality of service (QoS) functionality [20]. Figure 6 illustrates how the interframe space (IFS) and contention window (CW) affect the CSMA/CA protocol. Recall that a random slot is chosen from within the CW when a station checks the medium to see if it is clear to transmit, thus the larger CWmin the greater the delay will be before a certain access class (AC) could even have the potential to send. The sliding minimum and maximum values of the CW support QoS and the exponential increase back off of CSMA.

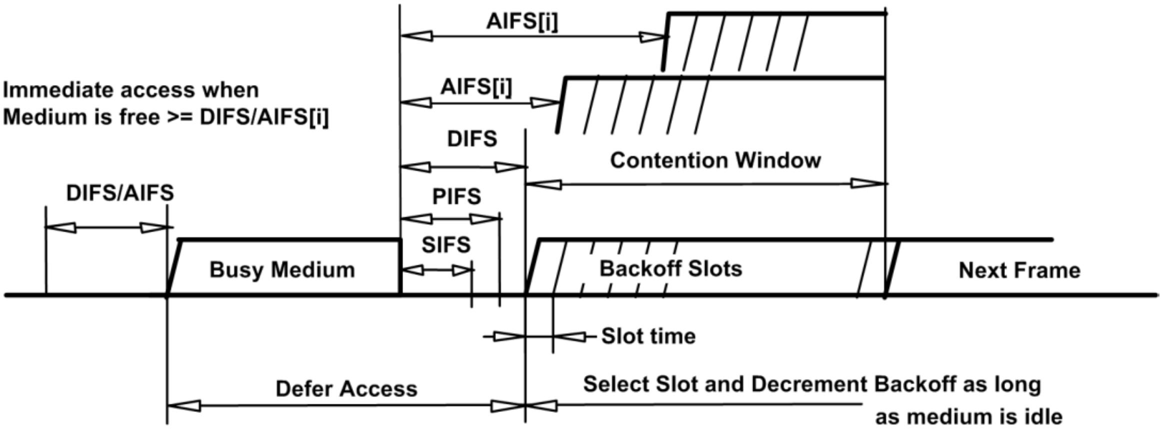
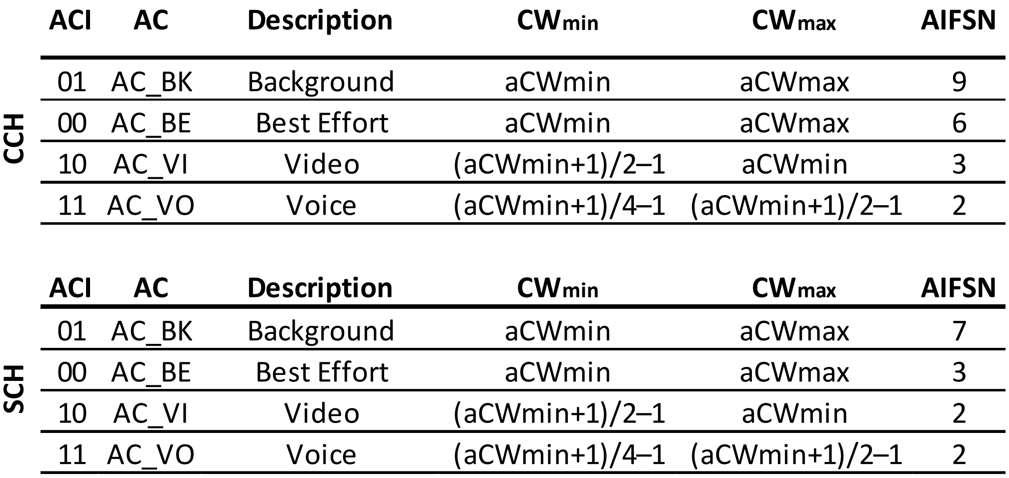


Figure 6. Frame spacing illustrated, source: [21].

Table 3. Default EDCA parameter set used in 802.11p [20].



	ACI	AC	Description	CW_{min}	CW_{max}	AIFSN
CCH	01	AC_BK	Background	aCWmin	aCWmax	9
	00	AC_BE	Best Effort	aCWmin	aCWmax	6
	10	AC_VI	Video	(aCWmin+1)/2–1	aCWmin	3
	11	AC_VO	Voice	(aCWmin+1)/4–1	(aCWmin+1)/2–1	2

	ACI	AC	Description	CW_{min}	CW_{max}	AIFSN
SCH	01	AC_BK	Background	aCWmin	aCWmax	7
	00	AC_BE	Best Effort	aCWmin	aCWmax	3
	10	AC_VI	Video	(aCWmin+1)/2–1	aCWmin	2
	11	AC_VO	Voice	(aCWmin+1)/4–1	(aCWmin+1)/2–1	2

Table 3 lists the values used in 802.11p for the minimum and maximum CWs and arbitration interframe space number (AIFSN) which is multiplied by the actual time slot (46 ms in DSRC assuming the normally used 4 ms guard interval which is the sum of the SyncTolerance and MaxChSwitchTime values [22]) and added to the time required to go from transmit to receive mode on a transceiver (known as the short interframe space, SIFS) [21]. This relationship is given in Equation 1.

$$AIFS[AC] = AIFSN[AC] \times aSlotTime + SIFS \tag{1}$$

IEEE Draft Standard 1609.0 (Draft 5 as of September 2012) [23] is being developed to describe the WAVE/DSRC architecture and services required for multi-channel VANET operation while IEEE Standard 1609.4 specifies the multi-channel capability of DSRC [22]. The 1609.4 Standard provides a mechanism to synchronize the participants and divide communications between the CCH that all units monitor and one of the six SCH that the various units choose to monitor [22]. It specifies, as shown in Figure 7, a fixed 100 ms sync interval comprised of approximately 46 ms monitoring the CCH, a roughly 4 ms guard interval, approximately 46 ms monitoring a SCH, and another approximately 4 ms guard interval. This multi-channel, distinct application capability of DSRC is a unique and interesting aspect of this networking environment. Work has been undertaken to take advantage of it in order to balance the desired safety and commercial services, as in [24].

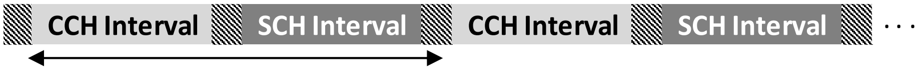


Figure 7. IEEE 1609.4 sync interval.

One of the innovations of the 2010 version of the 1609 standard is the permission for OBUs that have multiple physical layer devices, and only with those RSUs equipped to support, to agree on alternate channel monitoring schemes for secondary channels. Thus the primary physical device is required to monitor the CCH as before, but other physical devices on the same OBU are permitted to agree on the OBU staying on a CCH only, SCH only, switch between them, or simultaneously operate on the CCH and SCH with the multiple physical interfaces. Thus with multiple physical devices, secondary physical devices can be allowed to shift to a SCH in mid-interval, or skip a CCH all together and stay on the SCH. These are illustrated in Figure 8.

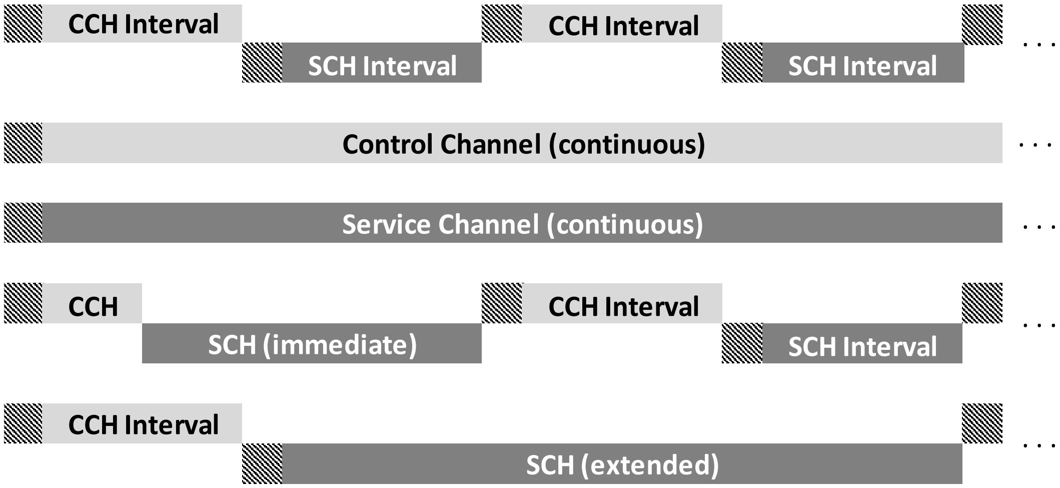


Figure 8. Channel access options: alternating, cont, immediate, and extended [25].

2.1.2 Network and Transport Layers

In addition to supporting the Internet Protocol version six (IPv6) network protocol using either Transport Control Protocol (TCP) or Universal Datagram Protocol (UDP) for datagram transport, DSRC also supports unique network and transport protocols designed for more immediate, single hop communication. These messages, known as WAVE Short Messages (WSM), are defined by the WAVE Short Message Protocol (WSMP) in IEEE Standard 1609.3 [25]. It is a simplified and extremely efficient means for exchanging information quickly between participants with very little overhead.

Of particular note is the security mechanism envisioned for VANETs as specified in IEEE Trial-Use Standard 1609.2 [26]. This installment of the 1609 family of standards calls for the use of a public key infrastructure (PKI) to secure the V2V and V2I wireless transmissions. It is also presently an area of great interest among academic, industry, and government researchers. While the idea of car communications has existed for many decades, the thought of securing the communications is a relatively new focus in only the last five or so years as pointed out in [27]. With the onset of a networked world, the increasing need for security has only become more apparent. Furthermore, there exists a fundamental belief that if this technology is to be implemented, no less than equivalent privacy must be provided by the VANET. A summary of the documented security considerations are provided in Section 2.2.

2.1.3 Application Layer

Upon standardization of the lower five network layers, it is assumed that most of the work going forward in terms of VANETs will be at the application layer. Two general applications are actually part of the 1609 family: 1609.1 which is a basic messaging service/resource manager [28] (but has been slated for potential withdrawal) and 1609.11 for electronic payments that could be used for tolls [29]. SAE J2735 specifies message sets, data frames, and elements to permit interoperability at the application layer. Some additional applications have been suggested by the IEEE DSRC working group and the Vehicle Safety Communications project and are listed in Table 4.

Table 4. DSRC potential applications [30, 31].

Public Safety

- Forward Obstacle Detection and Avoidance
- Lane Departure Warning
- Turn Accident Warnings
- Intersection Collision Warning
- Automated, Variable Message Signs

Transit

- Traffic Signal Priority
- Bus-Only Lane Enforcement
- Bus Turn Light Priority
- Automatic Fare Collection and Reporting
- Automatic Passenger Counting
- Route Optimization and Schedule Tracking
- Rider Information
- On-Demand Transit Services
- Security Systems
- Fleet Operations and Maintenance
- Many On-Board Systems ("Smart Bus")

Traffic Management

- "Smart" Traffic Signals
- Variable Message Signs
- Rapid Response to Incidents
- Enhanced Public Transit
- Central Traffic Management Center
- Electronic Toll Collection

Freight/Cargo Transport

- Vehicle Registration, Inspection, Credentials
- Route Guidance, Tracking
- Vehicle Monitoring, Inspection, Maintenance Systems
- Cargo Monitoring and Tracking (Including Multi-Modal Freight)
- Fleet Operations

Traveler Information/Support

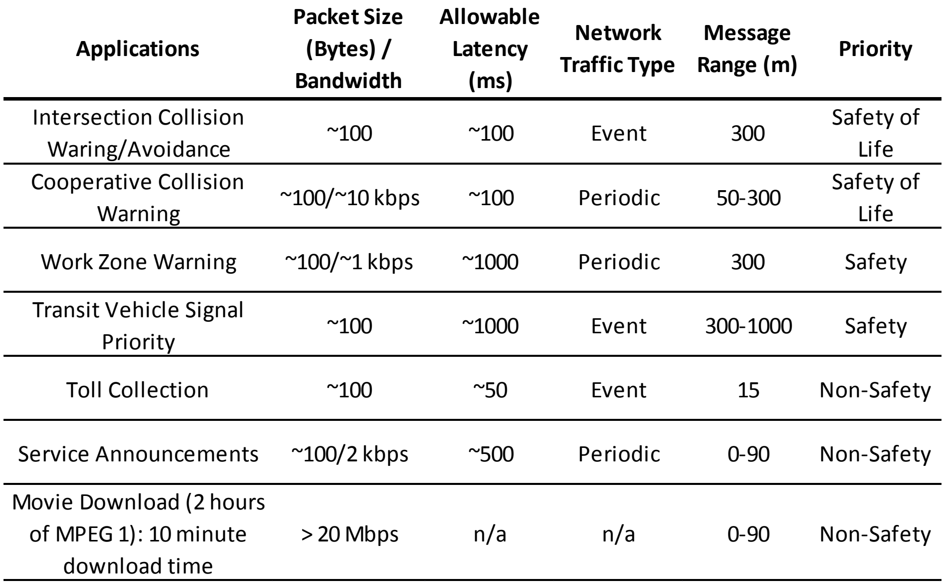
- Pre-Trip Planning
- Transit
  - Route and Fare Information
  - Schedule Information
  - Access to Personal Information During Trip
  - News
  - Weather
  - Internet Access
- Car
  - Navigation Aids
  - Traffic Information
  - Access to Personal Information During Trip

Automated Fee Collection

- Electronic Toll Collection
- Variable Road Pricing
- Parking

Various applications will have different traffic requirements. Table 5 lists different categories of applications and their corresponding data traffic requirements. It remains to be seen to what extent DSRC will support non-safety applications based upon OBU and RSU density and available bandwidth [18, 32].

Table 5. Typical DSRC data traffic requirements, source: [33].



Applications	Packet Size (Bytes) / Bandwidth	Allowable Latency (ms)	Network Traffic Type	Message Range (m)	Priority
Intersection Collision Waring/Avoidance	~100	~100	Event	300	Safety of Life
Cooperative Collision Warning	~100/~10 kbps	~100	Periodic	50-300	Safety of Life
Work Zone Warning	~100/~1 kbps	~1000	Periodic	300	Safety
Transit Vehicle Signal Priority	~100	~1000	Event	300-1000	Safety
Toll Collection	~100	~50	Event	15	Non-Safety
Service Announcements	~100/2 kbps	~500	Periodic	0-90	Non-Safety
Movie Download (2 hours of MPEG 1): 10 minute download time	> 20 Mbps	n/a	n/a	0-90	Non-Safety

2.1.4 VANET Distinguishing Factors

The previous paragraphs describe the makeup of vehicular networks. It is important to recognize that there are a number of characteristics that distinguish them from other networks, including [34-37]:

1. Vehicles (Nodes) have a Long Life Span (average 12 years [38])
2. Owners have Physical Access and Control over Nodes
3. No Technical Expertise is Expected from the Vehicle Drivers
4. Legal Aspects of Driving a Vehicle Complicate Situation (Liability vs. Privacy)
5. Low Tolerance for Errors in Some Applications (downloading a song involves little risk; if an error occurs in a VANET there is the potential for great risk to life and property)
6. Tension between Authentication and Privacy (need for some to know source; but desire to shield information from other users)

7. Many Safety Applications are Delay-Sensitive (if a vehicle in front slams on the brakes, one wants to know almost instantaneously so one can react)
8. Predictable (generally must stay on roads), High Mobility (speeds of zero to 85 MPH/135 KPH or greater) of the Vehicular Nodes
9. Highly Dynamic Topology (from widely variable speed of nodes)
10. Largely One-Dimensional Movement at Times (static road system; straight roadway legs)
11. Large Scale (covering entire cities, states, and potentially continents; there are about one billion cars on the road in the world)
12. Partitioned Networks (various entities certify various regions)
13. Vehicles not Completely Reliable (need for secure communication; nodes can break down)
14. No Significant Power Constraints (as in sensor networks)
15. Varied Density of Nodes (higher density in cities; lower density in rural areas).
16. Network Deployment (not all cars will possess VANET capability initially and there must be an incentive for vehicle manufacturers and buyers to desire its incorporation)

These differences contribute to a unique networking environment with new challenges to overcome.

2.2 Security and Privacy Consideration

Among these new set of challenges is that of security. While certain aspects of security remain unchanged, the unique VN operating environment alters other facets and introduces new considerations. Different aspects of VANET Security will now be examined.

2.2.1 Requirements [39, 40]

The security requirements in VANETs are no different from most situations. There is a strong desire for message authentication and integrity, which is the ability to know a message came from a purported source and the contents have not been changed. In addition there is the desire for message non-repudiation, which implies that the sender cannot deny that he or she is the source of the message. Entity authentication extends the receiver's knowledge to not only know who the originator of a message is, but also that the sender is presently active on the network/the message was sent fairly recently. Access control is the security property that assigns roles to various users and ensures that users are valid members of the network and operating in accordance with those roles, i.e. only performing authorized actions. Within a VANET it is also desired that some messages be able to achieve confidentiality, which means that only intended recipients of a messages contents are able to access it. Accountability is the security aspect that allows one to attribute events in the network to entities and users operating within the network. As with any network, availability is an important aspect for if the network is unavailable for use it might as well not exist.

Finally, privacy protection is a critical element of VANET security, which requires that protected personal information is not disclosed. Within VANETs this is related to limited or conditional anonymity such that other users are unable to authenticate the identity of the originator (but ultimately law enforcement should be able to when appropriate, such as a “hit and run” incident, which may or may not require a warrant depending on the policies implemented). Location privacy is a subset of this and entails preventing other users from tracking a vehicle. While privacy may not seem as critical to security as the other aspects aforementioned, it has consistently been identified among drivers, among the VANET projects, and in the academic-industry-government consortia as critical to VANET adoption [41, 42].

2.2.2 Vulnerabilities [43]

As with any network, if it is to be useful it must be connected to other nodes and in doing so the network becomes vulnerable to undesired nodes connecting. VANETs are no different and have a series of vulnerabilities as identified by the European Securing Vehicular Communications (SeVeCom) project. As a wireless network, it can be jammed, which means sufficient interference is produced that prevents reception of the actual signals. Forgery, the purposeful injection of inaccurate data as accurate, presents another hazard that could undermine a VANET. Furthermore, if data is to be transmitted beyond a single hop, the network becomes vulnerable to in-transit traffic tampering whereby other nodes can drop, modify, or resend messages. In addition to misrepresenting the payload of packets, an adversary could also impersonate a different sender. As the nodes are built into (or contained inside) vehicles, there of course exists the potential for tampering with the onboard unit itself. Finally, there exists the ability to learn not only who a user is, but also their actions and preferences resulting in a privacy violation.

2.2.3 Adversaries [37]

In order to understand the security dimensions of VANETs, there is value in considering the kind of people the most likely attackers might be. In general, there are five categories of adversaries a VANET may have to deal with. Greedy drivers may simply want an unfair amount of the bandwidth or to provide false information so they can direct traffic away from their intended path. Those who simply want more information than is due them are termed “snoops” by Parno and Perrig and could be simply engaging in voyeurism or scanning for opportune times to commit crimes. Pranksters are those with no direct benefit from their actions except potential notoriety from their success. Those from within the car industry seeking a competitive edge or financial profit through the abuse of their potentially more trusted position represent another adversary class and are termed industrial insiders. Finally there is the malicious attacker who consciously seeks to cause physical and logical damage.

2.2.4 Attacks [37]

These adversaries have an inherently large variety of attack vectors given the scope of VANETs and their wireless nature. Four general categories of attacks include denial of service (DoS), where the attacker simply seeks to shut down the network or node(s) from accessing the network. Message suppression attacks seek to undermine the connectivity of a network by dropping packets. Opposite of removing packets, fabrication attacks inject additional (and usually false) information into the network. Finally beyond simply adding or removing packets, the alteration attack changes the content of legitimate packets being sent.

2.2.5 Supportive Properties [37]

Fortunately for VANETs there are some characteristics that aid in providing security. As the OBUs are contained in vehicles, there exists the opportunity to regularly inspect the vehicle (and consequently the OBU) during annual safety inspections that are mandatory in most jurisdictions. This allows for validation of the tamper-proof device (TPD) assumed to be installed [43, 44], software updates, aid in the download of new certificates, and renew the current certificate revocation list (CRL). These last two items will be discussed more thoroughly at the beginning of Chapter 3. A second advantage is that most vehicles can be expected to behave correctly (honest majority). While of course this cannot be said to be always the case and especially not for a single instance where a malicious attacker is present. However for the many driver infractions that occur each day, there are many more responsible drivers on the roadway that, much more often than not, abide by the law. Thirdly, there are additional inputs to VANETs such as radar, light sensors, and of course the driver. Thus there can be more intelligence applied to the use of the information provided by the VANET. Another benefit to VANETs is the central registration that exists for vehicles to be placed on the road. Such administration should aid in the deployment of VANETs. The fact many portions of the road have controlled access (such as ramps on and off the highway or bridges to and from a city) make it easier to predict where the majority of vehicles will travel. In addition to pre-existing administrative support to define the VANET, there are also existing enforcement mechanisms, namely the police and other law enforcement entities that can allow for better arbitration within the VANET.

2.3 Proposed Methods of Balancing Authentication and Privacy

In VANETs, there is an inherent need for trust due to the interdependent nature of the nodes participating in the network. The safety of one vehicle and its reaction to emergent information received is dependent upon its ability to trust that information. If a vehicle reports a car in fog in front is slamming on its breaks, a vehicle has a split second to decide how it is going to respond to this information. Multiple means of organizing these trust methods, with various levels of authentication and privacy have been offered. In [45], these are divided into two categories: those that are infrastructure based and those that are self-organizing. Infrastructure based trust approaches involve establishing trust through some external, mutually trusted entity and include certificate-based systems as well as blind signatures, proxy signatures, and group signatures. Self-organizing based approaches require the autonomous evaluation by each node regarding whether to trust any other node and are known as reputation based systems.

There is vigorous debate as to the better approach to securing vehicular networks. While many researchers have investigated self-organizing methods [46-51], the IEEE 1609 standards body has maintained a preference for an infrastructure based system due to the legal and safety implications involved. Relying on external, unknown entities to "vote" on whether to trust another vehicle provides too great a safety vulnerability as it is exceedingly easy for a rogue group to conspire to bias the trust levels of any reputation-based system – or even a single person with multiple identities (which is a Sybil attack).While it is quite possible that the various self-organizing systems could have impactful use for various applications (such as restaurant and product reviews), it remains envisioned that an infrastructure based system is necessary to meet legal requirements and provide the highest level of system confidence. Reputation-based systems definitely have the potential to enhance security, but due to the limited contact any two nodes have with each other and the privacy implications involved, it is generally not considered a good basis for VANET security.

In terms of infrastructure based systems, considerable energy has also been expended examining various methods to secure VANETs and provide for authentication and privacy. While there is much consensus that a PKI is the best solution to providing security (including privacy as soon discussed) to VANETs, alternatives have been proposed primarily out of motivation that a PKI is too complex to administer (including the difficulty in distributing PNs) [52]. Identity-based encryption was proposed in [53], but has not gained much following as the vehicle is given the opportunity to build as many identities as possible opening the network to Sybil attacks and vehicle identities must be pre-distributed. Group signatures have been suggested, such as in [54, 55], but are computationally expensive given that the key must change (requiring RSU access) every time a new vehicle enters or leaves a group and the short duration of groups that is expected given the ephemeral nature of VANETs. Hu and Laberteaux present in [56] another approach where messages are sent encrypted but the keys are sent later, but this approach raises the question of what to do if the key is never received or if the delay in receiving the key is too great to take the appropriate action. OBU-generated certificates that are then signed or blindly signed by a CA have also been proposed as in [57], but this doubles the amount of data to be transmitted and questions arise over OBU's generating their own certificates.

Golle, et al, propose doing away with any message signing and relying solely on sensors to provide VANET security [47]. They envision each vehicle creating an entire model of the VANET via its sensors and then using this model to determine if messages it receives are valid. This undermines the cooperative nature of VANETs and greatly limits its value to the limited range of a vehicle's sensors. Another approach to message security is proposed in [58] in which all messages received are submitted to an RSU for validation. This depends on a large density of RSUs and again is inefficient in its requirement for additional bandwidth. Thus others have sought to abandon the PKI approach but shortcomings have kept the bulk of academic, industry, and government research and standardization efforts on implementing a PKI, recognizing the need to adapt it to the unique vehicular environment.

2.3.1 Public Key Infrastructure

PKIs are generally comprised of three entities: users, certificates, and the certificate authority (CA) [59]. In our case, the users are the on board units (OBUs) within the vehicles and the road side units (RSUs) that are deployed. The certificates are what bind an entity to an identity and their formats are specified in RFC 5280 and referred to as X.509 PKI Certificates [60]. The CA is who issues the certificates that implement a hierarchy of trust. The CA is often referred to as the "root" for if one has its public key, one is able to establish trust down a chain of certificates to the entity in question.

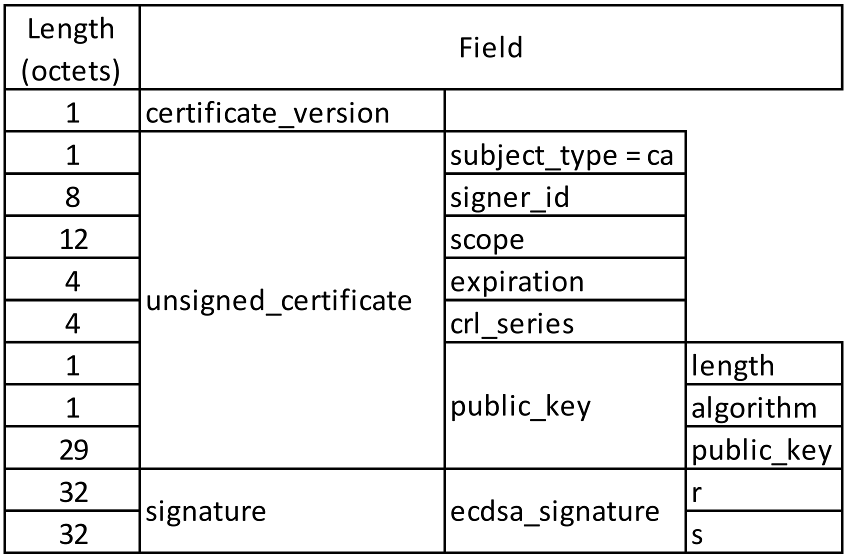
As laid out in section 2.2.1, VANETs have a number of security requirements. It is envisioned that PKI would be the “trust anchor” for VANETs [44]. In fact, the Trial-Use IEEE Standard 1609.2 covers security within VANETs and codifies the use of a Public Key Infrastructure (PKI) for the securing of vehicular communications with corresponding definitions given under section 5.15 [26]. Sections 5.11 and 5.12 of IEEE 1609.2 dictate the use X.509 certificates using the elliptic curve digital signature algorithm (ECDSA) as presented in Federal Information Processing Standard (FIPS) 186-2 [61].

CHAPTER 3

VEHICULAR PUBLIC KEY INFRASTRUCTURE

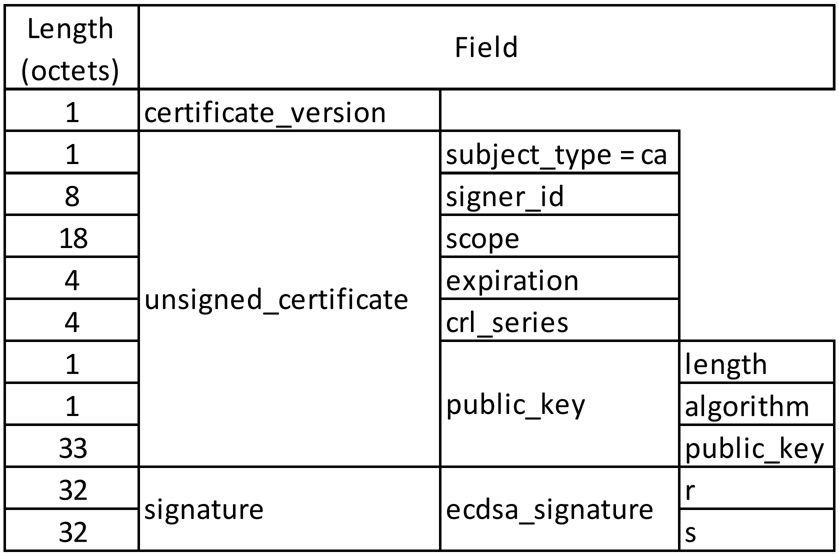
The problem of protecting a user's privacy while ensuring the ability to attribute abuse in VANETs remains open and important to solving the engineering challenge that is networked vehicles. As discussed in Section 2.3, while other approaches have been offered in the literature, the standards have consistently adopted for use a PKI and the research community has recognized the need for implementing pseudonymous certificates to protect the privacy of VANET users [62, 63]. However, the underlying assumption has been to utilize a long-term root certificate authority (CA) key to perform the signing. In our work, an alternative technique designed specifically for the use in networks of an ephemeral nature is proposed. Our proposed technique solves the problems of a reduced key space and "wasting" of certificates (as discussed in [64]) while providing insight into the logistics of a VANET PKI (VPKI) implemented within a regional framework. Work by others assumes a large VANET infrastructure (with the ability to contact the certificate issuer at any time) that does not exist (and will take considerable resources to build) [62, 65]. Our approach requires less additional infrastructure compared to these approaches. Without a doubt, a traditional PKI must be adjusted [66] to work in a vehicular environment based upon the network and legal differences highlighted in Section 2.1.4. For example, since an always on connection does not exist in a VPKI, two of the most important aspects of a traditional PKI are hindered: the distribution of new key pairs (pseudonyms in a VPKI) and the distribution of certificate revocation lists (CRL). A method that solves the latter challenge is provided by Nowatkowski in [67]. The former challenge remains an open problem and is the focus of this completed research.

In terms of IEEE 1609.2, certain parameters of VPKIs have been set including certificate details. The OBUs (which are assumed to have less processing power) are specified to use 224 bit keys while the CA and RSUs are specified to use 256 bit keys. Annex C of 1609.2 provides the structure of the certificates and specifies 125 byte OBU (see Figure 9) and 135 CA/RSU signing certificates (see Figure 10) [26]. A pseudonym consists of the certificate (which proves the validity of the sender) as well as the sender's public key (which is used to validate the signature for integrity purposes). Thus an OBU pseudonym is 153 bytes (29 bytes for the public key and 125 bytes for the signature).



Length (octets)	Field		
1	certificate_version		
1	unsigned_certificate	subject_type = ca	
8		signer_id	
12		scope	
4		expiration	
4		crl_series	
1		public_key	length
1			algorithm
29			public_key
32	signature	ecdsa_signature	r
32			s

Figure 9. OBU certificate (adapted from Figure C.2 in [26]).



Length (octets)	Field		
1	certificate_version		
1	unsigned_certificate	subject_type = ca	
8		signer_id	
18		scope	
4		expiration	
4		crl_series	
1		public_key	length
1			algorithm
33			public_key
32	signature	ecdsa_signature	r
32			s

Figure 10. CA certificate (adapted from Table C.1 in [26]).

3.1 Pseudonyms

It is through asymmetric cryptography that all of the security requirements are met, with the sole exception of privacy. In order to achieve this requirement, Hubaux et al. introduced the idea of using multiple certificate pairs in VANETs in [68], which they termed “pseudonyms” (PNs) and proposed to measure anonymity via an entropy-based approach. A public key infrastructure where multiple keys are issued to vehicles for use in signing messages is known as a vehicular or VANET PKI (VPKI). In [69], the author of this proposal lays out the foundation for a VPKI that supports up to one second PN shifts, includes regions, the periodic recycling of the PN key space, and PN assignment strategies to improve VPKI administration.

Pseudonyms are the key component to bringing privacy to VANETs and have been identified as the best approach to securing VANETs [70]. By changing the certificate used in signing a message, it becomes impossible to link two transmissions based solely upon the keys used (which is not the case for a standard PKI where the private key, and subsequently the public key, do not change). PNs will be an important part of VANETs and only as implementation becomes a reality and IEEE 1609.2 matures will these parameters and their effects on network functionality (such as routing as discussed in [71] where changes of one minute had minimal impact while changes of five seconds or less undermined routing) and security be fully understood and established.

3.2 VPKI Privacy Enhancement

The literature lays out a variety of other methods to achieve and/or improve privacy. It remains to be answered how often pseudonyms will change, how many PNs a vehicle will possesses at any given time, and how often this pool of PNs will be refreshed. In [72], the changing of PNs is recommended to occur based upon speed and existence of neighboring cars, the idea being that the slower one is going or the fewer vehicles nearby, the less often changing one's PN increases privacy. The idea of "mixed zones" is presented in [73, 74]. This extends the "neighbor" concept to fixed geographical places that when cars all enter a certain area (zone) then all the vehicles change PNs simultaneously so an outside observer who is watching a car enter the zone would no longer be able to determine who the car is when it leaves the zone. In [75] a protocol entitled "CARAVAN" is presented that groups nearby vehicles into a caravan such that random periods of silence are enforced on the vehicles and a subset of the vehicles in the caravan report their position and velocity information since they are all close together and have similar characteristics. Eichler in [76] extends the silent periods to a more general “quiet time” rule that requires vehicles to enter a period of no transmissions prior to changing their PNs to prevent observers from linking PNs.

3.3 Factors that Affect Pseudonym Use

As discussed in Section 3.1, pseudonyms are a critical component to implementing a VPKI that meets all the security requirements (outlined in Section 2.2.1) *including* providing privacy. It is important to note that the actual details of PN usage remain to be established. There are a number of these details that are necessary to consider when designing a VPKI. One of these is storage. If PNs are going to be generated by the trusted infrastructure, in order for this trust to be preserved there must be secure storage that prevents tampering with the vehicle’s private key(s) and the PNs themselves (so that they are not misused in signing messages that do not originate from the vehicle). Thus a trusted computing platform (TCP) as discussed in [77] or its equivalent is a necessary development before the deployment of truly secure vehicular networks. In addition to have secure storage, there must also be enough. With the plunging cost of storage per gigabyte, this is not considered to be a problem [78].

Another factor regarding PN use is the duration for which a single PN is valid. A related and slightly different question is for how long a particular PN will be used and whether multiple PNs will be valid over the same period. The literature suggests the lifetime of a pseudonym to be from a second to a minute to a few minutes to a day or longer [36, 79]. Eichler in [76] claims that 100 seconds is the best choice. Whether or not these change times should be static or dynamic [76, 80] or be geographically bound [39, 81] are also under consideration. There is also the question of how many certificates should be on an OBU in terms of covering all 24 hours of the day or less time given cars are not on the road around the clock (which would also affect storage).

Another important factor is how often an OBU is envisioned to go between downloading additional PNs as well as the maximum time an OBU is allowed to go without infrastructure contact and PN refill before it lacks any valid PNs. The more often it needs to contact the infrastructure, the less PNs it requires each time and storage space it requires, but the greater the burden on the infrastructure (in terms of deployment density) and less bandwidth available for other applications. The results from an analysis we did in [69] are shown in Figure 11 which illustrates the relationship between storage (y-axis), PN refill period (x-axis), and PN use duration (plot lines).

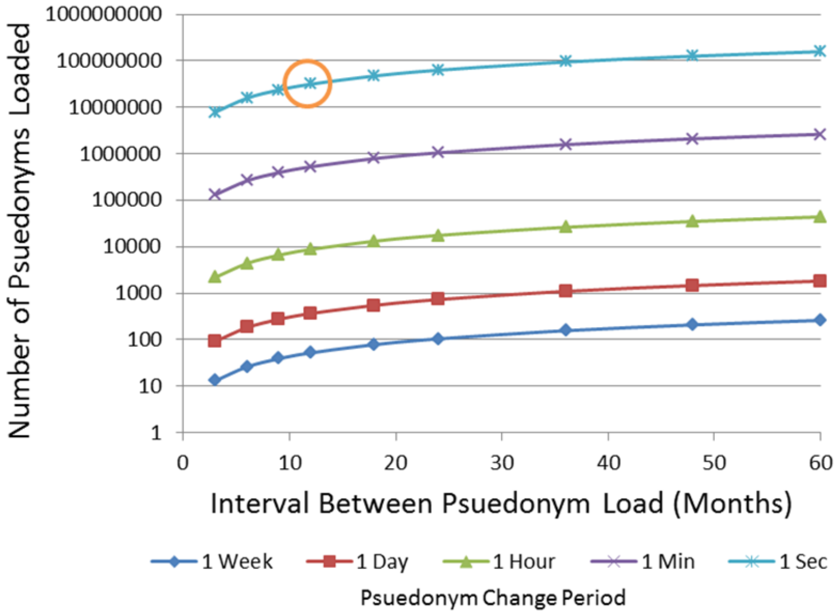


Figure 11. Relationship of pseudonym shift and reload period.

When discussing any PKI, it is imperative to allow for the revocation of certificates which can occur for a variety of reasons. In a VPKI, a car could be sold, stolen, or suffer a system failure, each of which would result in the need to cancel the validity of the remaining certificates. The more certificates that are generated and distributed, the greater the demand placed on the revocation process. One solution to revoking VPKI certificates involves the use of certificate revocation lists (CRLs) [82]. Efforts to improve the efficiency of CRLs for VANET applications are presented in [83].

3.4 Use of Regions within a VPKI

One of the fundamental building cells of any public key infrastructure is the certificate authority, the ultimate gatekeeper in whom all entities of the infrastructure place trust in. We envision in our work [69] that VANETs will be dissected into geographic subdivisions known as regions. These regions are of two different varieties: those which are subdivided within a given CA which are called "intra-regional entities" and those that cross CA boundaries which are called "inter-regional entities."

The authority that can establish and revoke keys below a root CA is known as a regional certificate authority or simply RA. Provided that there is a balance between the number of intra-regional entities, then it becomes possible for an OBU to possess all of the RA certificates or at least those that are closest and most likely to be encountered. If such an OBU enters an intra-region without that RA's public key, then it will have to request it from an RSU it encounters (ideally) or another OBU (if necessary). Since the RA's public key is signed by the root CA which is already known to the OBU, there is no potential violation of trust outside those inherent to the use of a PKI (such as the root CA's private key being compromised).

3.5 Inter-Regional Operation

In our work [69] we point out that the implementation of a vehicular public key infrastructure is slightly more complicated than the intra-regional scenario because the OBU would **not** normally possess the public key of the external CA. This scenario can be resolved in multiple ways, all of which ultimately result in the same technical result from the OBU's perspective. One option for trusted international partners might be to simply "cross certify" the root CAs. In this case, each root CA signs the public key of the neighboring root thereby assimilating all the neighboring OBUs into its VPKI. Then when sending interregional messages, the OBU must also send the public key of its domestic root CA. The receiving OBU can then either add an additional step of confirming the sender's root CA public key and then use that to verify the sender or if such a vehicle has already encountered a foreign vehicle from this same root CA and possesses that key, can immediately verify the trust of the sender and read its message.

In the case where the root CAs are not ready to provide full trust to a neighboring region, a method of "guest registration" must be implemented. This could be performed in advance before arriving at the border by requesting a single or multiple PNs for use in the foreign region depending upon their policies or at the border crossing itself during the typical customs inspection. Thus travel within the United States or Europe could be considered intra-regional while crossing from Texas to Mexico or from a Schengen country to the Ukraine would be inter-regional and require these extra processes.

However once an OBU is granted guest PN(s) it would function in the foreign region just like any other OBU within that region.

3.6 Overview of a Framework to Support Frequent Pseudonym Shifts [69]

Vehicular ad hoc networks (VANETs) provide the means to add convenience, services, and safety to the road. We now introduce our work [69] as a means to adapt the concepts of Public Key Infrastructure for a VANET environment under the worst case scenario of a pseudonym shift every second. Regions are used to scale down the size of certificate revocation lists (CRLs), administrative overhead, and the search space to link a message to its originator when necessary. Regions also provide a means for expansion of the geographical area covered and provides the ability to balance geographic mobility with privacy. Whereas previous discussions have been in general, what follows is one particular example we have developed of how a VPKI could be implemented, outlining our method to extend PKI to VANETs. What follows provides the details for the infrastructure itself as well as the method of issuing pseudonyms to maximize privacy, ensure attestation, and develop an exceptionally large pool of private/public key pairs to draw from. This framework can then be modified to the decided pseudonym shift frequency and/or extended for other purposes.

In a VANET, two distinct components comprise the communication infrastructure: onboard units (OBUs) and road side units (RSUs). OBUs reside on the vehicle and possess reasonable, albeit limited, computing (i.e. processing, memory, storage, etc.) power. Such units are mobile and thought to be very large in numbers and the primary communicators of the system. RSUs, on the other hand, are fixed structures, networked together with access to the CAs, which can provide greater computing power and can be used to administer the network.

In a PKI, a chain of trust is established between two users by a mutually trusted entity (ultimately the root CA). When Internet access is present, the trust chain can be traversed with little effort provided the public keys of all intermediaries between the root CA (which, it is assumed, is already trusted by both parties and that both parties are in possession of its public key) and the entity to be confirmed is available. If the public keys of the intermediaries are not already held by the verifier, they are normally available for download within the PKI certificate directory.

The dynamic shifts considerably when Internet access is not assumed (as in VANETs) which results in being unable to acquire missing public keys on demand. It is for this reason that the originator of a message includes his or her public key when sending signed messages [26]. Thus the receiver will have the public key of the message's originator and needs to have the key of the root CA and any intermediary authorities. How many CA/RA keys are needed and how these are acquired is what this section answers.

To minimize the number of CA/RA keys needed, balance security of the root CA, minimize the processing required to verify keys and validate messages, and provide for a virtually unlimited number of keys, a relatively flat PKI hierarchy is proposed to be used, even flatter than the supported five layers of IEEE 1609.2 [26].

3.6.1 A Note on Sybil Attacks

The current draft IEEE 1609.2 standard OBU and RSU certificates only have an expiration date and no start of validity of date. Thus if many certificates are provided under the current standard, an OBU would have a large number of valid certificates at the start which trailed off in time. As discussed in [84], we concur that the standard should be amended to have both a start and stop date for validity which reduces the number of valid certificates at a present time (down to one should it be desired) and thus reduces (and potentially eliminates) the possibility of a Sybil attack. This is the result of limiting the number of issued certificates that are valid at any given instant, which, at one extreme, can be one (thus eliminating Sybil attacks altogether). Should the number of issued and valid certificates be greater than one, it would be necessary to detect malicious behavior such that an OBU that participates in a Sybil attack would have all of its certificates revoked [47, 85, 86].

3.6.2 Vehicle Identification Number Certificates

When a car is manufactured, a unique vehicle identification number (VIN) is assigned to the car by the manufacturer (and administered by a political authority such as the U.S. Department of Transportation). When a vehicle is first titled, an identity certificate is issued binding this VIN to the OBU, similar in function to the electronic chassis number discussed in [72]. The OBU is assumed to be a tamper-proof and secure computing platform. While this certificate is permanent (it resides with the vehicle, not the owner), it is only used for communications between the OBU and the CA. This portion of the scheme reflects a traditional PKI. The root VIN CA certificate should have crypto periods of 30 years and the root VIN Extended CA certificate should be valid for 10 years in keeping with current best practices [87]. This means that about every ten years the VIN-binded certificate will have to be renewed. Again, such logistics fall under the domain of a traditional PKI.

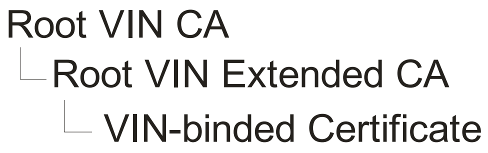


Figure 12. Certification path for vehicles identification number-binded certificate.

3.6.3 Root and Regions

For a given nation (ex. United States) or political entity (ex. European Union), a single root CA (complementary but distinct from the root VIN CA) is established. Subordinate to the root is a series of regional CA’s (an example of regions for the United States is provided in Figure 13). The root CA signs the certificates issued to the regional CAs who in turn use these certificates to sign all pseudonyms issued in a given region (see Figure 14 from our work in [69]). The root CA is only used to sign the regional CA’s certificate every nine months (this will be explained next).

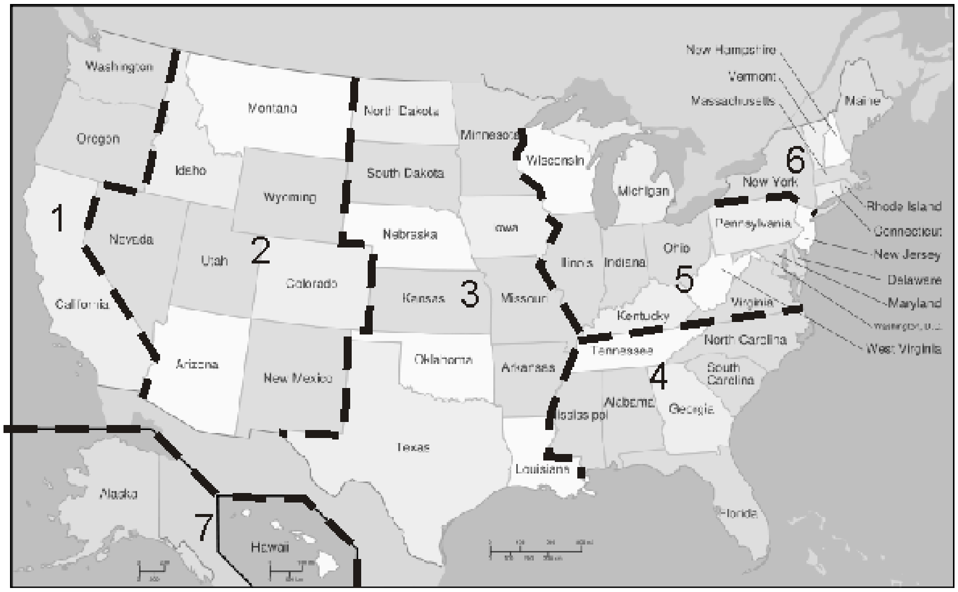


Figure 13. Example of potential regions in the United States.

It is worth noting that the Root Class 2 CA also signs a Regional CA to be used by the root for issuing certifications that are valid throughout all the regions but at a decreased level of privacy. Privacy is reduced because a limited number of cars will be using these “universal” certificates and thus they will be easier to track. This CA is used to issue pseudonyms to international vehicles, commercial vehicles that routinely drive across multiple regions, and vehicles titled outside any regional authority (ex. military or federal).

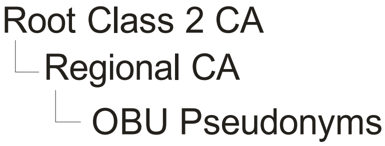


Figure 14. Certification path for OBU pseudonyms.

3.6.4 Vehicle Registration

Each region then serves as a subordinate (Regional) CA to whom each political subdivision, which we will refer to as territories, serves as registration authorities (RAs). When a vehicle is titled in a territory, that territory's motor vehicle department verifies the car's identity (using the VIN certificate) and then requests a block of pseudonyms from the regional CA. The block consists of certificates to be used over, for example, 12 months (the exact number of pseudonyms is dependent upon the rate they are elected to change; we are assuming a worst case scenario of one per second and certificates for every second of the day).

To further improve security, the blocks of certificates are limited in their validity to some subset of this time, such as one week or one month (or even one second). This reduces the likelihood of flooding the roadways with valid certificates and ultimately results in a reduction in the size of the certificate revocation list. In addition to the pseudonyms, the complete set of valid public keys for the root CA and all regional CAs must be downloaded to the OBU. As will be seen shortly, this will require 3n public certificates, where n is the sum of the number of regions under the root plus two (one for the Root Class 2 CA and one for the Regional Root CA).

Vehicles then perform this registration annually (much like paper registration) at either a government office or a contracted registration office. Such offices would have VPN connectivity to the RA and simply serve as the secure conduit. Renewals of pseudonyms would ideally occur seamlessly. In Pseudonyms on Demand [65], it was proposed that a user could refill pseudonyms continuously at local RSUs. However this assumes a tremendous (and costly) infrastructure is in place.

3.6.5 Certificate Term of Validity

Here lies the novelty of our scheme. Unlike traditional PKI, a PKI within a VANET construct must be formed differently. No longer can the root certificate have a lengthy term of validity for this will result in large search scopes. Likewise, one must also eliminate an extensive certification path to ensure each OBU has the corresponding CA public keys.

We propose that the root CA stores the necessary information to link certificates with the issuer so as to be able to identify a user and provide traceability. Thus, the same key pair can be re-used provided a different CA issued it. Furthermore, the root CA and regional CA keys must be generated in advance and sufficient time provided to ensure they are distributed to every OBU.

The root and regional CA public/private key pairs exist through three phases. At the beginning of the first phase, the keys are generated and then during the remainder of this phase the public key is distributed. During phase two, the public key is distributed and now the private key is used to generate the pseudonyms which will become valid at the start of phase three. In the final phase, the public key is still distributed and now the pseudonyms become valid for use. For a given key pair, these three phases represent one key cycle. The keys cycle based upon the following constraints and an example is illustrated below. Furthermore, Table 6 and Table 7 summarize the actions taken in each phase.

Table 6. Phase activity by registration authority.

RA (If CA cert series is…)	Distribute CA Public Keys	Issue OBU Pseudonyms	Pseudonyms Valid
Phase I	Yes	No	No
Phase II	Yes	Yes	No
Phase III	Yes	No	Yes

Table 7. Phase activity by on board unit for a single key series

OBU:	Receive CA Public Keys	Receive Pseudonyms	Use (Valid) Pseudonyms
Phase I	No	No	No
Phase II	Yes	Yes	No
Phase III	No	No	Yes

The third phase lasts for the overall duration of the validity of the key block issued. The time for which renewals are permitted prior to the key block expiring is the duration of the second phase. The first phase lasts the length of the third phase minus the length of the second phase (Equation 2).

The number of overlapping key pair cycles (OKPC) is given in Equation 3. This also represents the number of public keys an OBU must store for a single RA key pair.

$$\text{Length of Phase I} + \text{Length of Phase II} \equiv \text{Length of Phase III} \tag{2}$$

$$OKPC = 2 \times \left\lceil \frac{Length\ of\ Phase\ \mathrm{III}}{Length\ of\ Phase\ \mathrm{II}} \right\rceil \tag{3}$$

From the OBU's perspective, on its initialization in the system, it would receive all the public keys from the series in Phase I, II, and III. Its pseudonyms would be generated from the single regional CA in phase II. For renewals, it would only need to receive its pseudonyms (from the regional CA in phase II) and the public keys from the CAs in phase III for use in subsequent cycles.

For example, pseudonyms could be issued in 12-month blocks with the earliest renewal six months prior to expiration. This would mean the “future” public keys would have to be advertised six months in advance. Thus phase I would be six months, phase II six months, and phase III twelve months long. The root certificate would be generated and in use for 24 months, valid for 18 months, and only used to issue pseudonyms for six months. The first six months would serve as the distribution phase (I), the next six months as its active use for issuing new pseudonyms (II), and the final 12 months of its validity would be its sunset phase (III). In the sunset phase the OBU certificates previously issued are valid but the number of valid certificates stored on all OBUs gradually reaches zero. Thus every six months, the set of available pseudonyms returns to its untapped, maximum size.

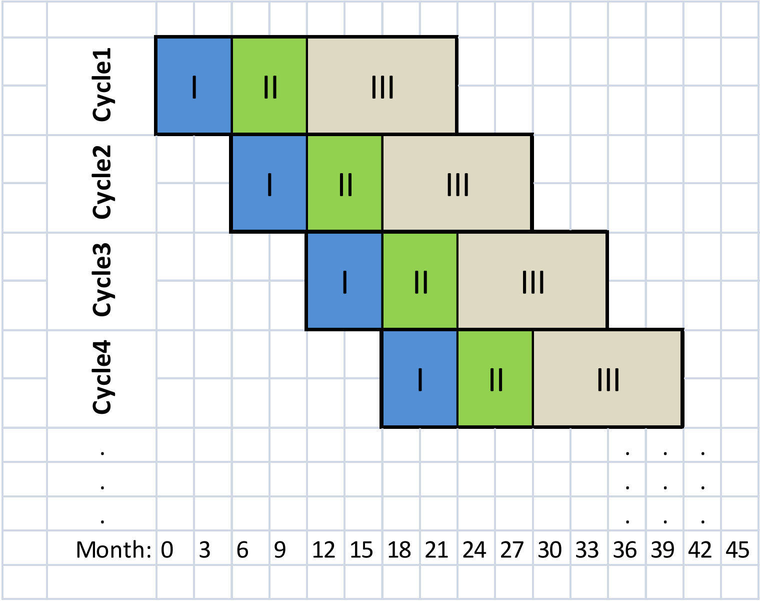


Figure 15. Root and regional CA cert. lifespan example (showing cycles).

3.6.6 Pseudonym Shift Frequency

The pseudonym shift frequency remains one of the most critical design criteria yet to be determined. In [55], a one minute interval is used and in [63] pseudonyms are changed every 10 minutes. Others, such as in [53], use a user-defined interval. The rate of pseudonym shift directly impacts the number of pseudonyms provided at a time (see Figure 11 on page 33). The other factor is the period between refills – longer periods require more pseudonyms per refill. At present, we are assuming a static refill based on a one year period. Future developments hope to follow others [65] in relying upon actual consumption to determine the number of pseudonyms provided but without the reliance on expensive (and as of yet non-existent) infrastructure.

3.6.7 Region Development

It is envisioned that VANETs will deploy in a progressive fashion. This scalable scheme is very flexible to grow and shrink provided regions do not get too big and overload the CA or too small so as to make distributing the regional CA certificates too inefficient. To add a new region, a new regional CA would be established and its public key would be distributed along with all the other regional public keys six months prior to it signing new keys (during phase I). The rest of the process would continue as before. Note that after 18 months of its first distribution, "n" of Section 3.6.4. increases by one for each additional region.

To remove a region, one simply does not distribute any more public keys for it and then use the region keys associated with the region(s) that cover the previous region. In our example, this results in "n" reducing by one after 18 months.

3.6.8 Inter-Regional Pseudonyms

Within the area covered by the root CA, vehicles are able to travel between regions (e.g. when taking a trip). Likewise, people who live on the border of two regions are likely to spend time within both regions.

It is a privacy concern for a vehicle registered in region 1 to be travelling in region 2 as the set of vehicles with pseudonyms signed by an outside region is significantly smaller than that of those signed by the present region. To resolve this, we propose assigning pseudonyms on a fractional basis from neighboring regions such that at least a third comes from a neighboring region but no less than half come from the primary region. For example, vehicles registered in region 1 would receive 2/3 of the pseudonyms from region 1 and 1/3 from region 2; vehicles registered in region five would receive 50% of the certificates from region five, and 1/6 from regions three, four, and six. This allows for a mixture of regionally assigned pseudonyms to be used in a given region (so even vehicles registered in region one will sign using region 2 certificates) and the use of more than one region by a vehicle (so when a car from region one is in region two, it can use predominantly region 2 certificates).

Should a vehicle travel beyond neighboring regions, it will have to perform a “visitor registration” which can be done over the DSRC channel. Such registration would involve communicating via RSUs using the VIN ID certificate and acquiring a small (e.g. one week’s worth) number of pseudonyms for use while in that region. This is similar to the inter-root CA process outlined below, however is greatly simplified due to the common root CA.

Recall from section 3.6.3 that a mechanism also exists for vehicles that routinely cross regions to have its certificates issued by the root CA at a decrease in privacy.

3.6.9 CRL Considerations

Two CRL choices include the traditional list and a Bloom filter. Under the traditional CRL, each region maintains its own CRL which it periodically transmits as described below. A window of time is used to determine who to include in the CRL (for instance, if a vehicle is revoked with six months of certificates left with a shift frequency of one second, only the next week or two would be added to each CRL distributed). Certificates that have expired are simply removed from the CRL by both the OBUs and the CAs.

An alternative was introduced by Haas, et al. to use a Bloom filter to reduce the size of the CRL and expedite an OBU verifying a given certificate has not been revoked [63]. We extend this idea to encompass the use of regions. Each region will have its own CRL. Furthermore, the CRL's are self-pruning due to the certificate expiration dates and revoked certificates that are not yet valid would not be included in the CRL. The processing required to build the Bloom filter bit vector is handled by the RAs.

The distribution of a CRL is covered in [84]. In a given region, the CRL bit vector would be transmitted on the first service channel (SCH) as needed, but at an interval no greater than 12 hours. The CRLs of the other regions would be transmitted on other service channels based on geography (ex. the region to the north on SCH 2, to the east on SCH 3, etc). The root CRL (to handle international vehicles) would be transmitted on SCH 6. Recall from Section 3.6.7 that vehicles operating in a given region are required to use pseudonyms produced by that or an adjacent region, thus there is no need for a vehicle to have a CRL from a non-adjacent region.

There is a trade-off between the size of the CA region and size of the CRL, as well as the management complexity of the entire PKI system for VANETs. The least complicated region to manage would be a single large area, such as the entire United States, with a single CA responsible for every certificate and pseudonym. This would also result in the largest CRL since every revocation would appear on the CRL. This relationship can be summarized as: (a) the CRL size is proportional to region size and (b) the management complexity is inversely proportional to region size.

Bellur in [88] gives some analysis on region size and provides some techniques for managing transitions from one region to another. Thus, a vehicle would have a set of pseudonyms for their "home" region plus additional sets of pseudonyms for regions adjacent to their "home" region.

3.6.10 Archive Implications

To maintain traceability of a given message with included public key, the regional CA must maintain a database of the issued public keys by a given regional CA (and potentially the expiry date) to each VIN. The size of this is determined by the change rate of the pseudonym. There is no need to keep the private key provided one can rely on the principles of asymmetric cryptography (i.e. one accepts that the odds of another private key producing an output that can also be unlocked by the provided public key approaching zero for sufficient key length).

The size of the data to be archived can be reduced through the use of hashes. By hashing the key, one reduces the amount of information to store, but one also reduces the ability to uniquely match a public key. However this may be more politically viable as it increases privacy while providing statistically significant matches. Furthermore, a decision must be made as to how long to keep these records in terms of a statute of limitations, such as twenty years (the longest timed length for federal crimes in the United States [89]).

3.6.11 Inter-Root CA Travel

Another area of limited development is the movement of vehicles between areas covered by different root CAs (which was introduces in Section 3.4). Along those borders of countries with strong diplomatic ties, mutual trust, and equivalent standards, cross certification can be employed as previously discussed.

On borders where this is not the case, a temporary vehicle registration process could be set up so that upon entering, a vehicle is registered with the root (a temporary VIN certificate can also be issued if not present or not compatible), the root and regional CA public keys can be provided to the vehicle, and a block of pseudonyms can be issued sufficient for the length of stay, all consistent with the general principles previously set forth.

3.7 Overview of Preliminary Pseudonym Distribution Protocol [90]

Using our work from [69] as an established framework to provide some sense of a canvas to work with, we now turn to examining our work on how PNs might be transmitted from an RSU to an OBU. Having VANETs support this methodology of PN delivery is critical for mass adoption of VANETs given the magnitude of the scale of motor vehicles. In this section we present a method of pseudonym distribution that works across regions. This methodology can also be used for the efficient refill of pseudonyms within a region thus simplifying the acquisition of pseudonyms to a single, standardized protocol regardless of the scenario.

Other works have investigated the need for privacy through PNs and their efficient use. Some of these papers have focused on completely anonymous transmissions [91, 92] at the expense of authentication and thus security. Some papers have focused on strengthening the privacy within a VANET by altering the pseudonym switch behavior (as in [93]) or the antenna characteristics (as in [94]). In [62], the authors introduced a method of using anonymous certificates to acquire pseudonyms (PNs) in other regions. While these certificates could be verified to be valid, the assumption is that the other region would find issuing certificates to an anonymous, albeit verifiably valid, user acceptable. Most nations insist on authenticating a traveler crossing the border (ex. via passports) and thus this scheme does not seem acceptable to traveling across regions of different jurisdictions. There is little discussion in the literature of the details of actually exchanging PNs within a VANET between an OBU and an RSU. This section attempts to fill this void and may even be used with the various PN approaches found in the literature (including the ones previously discussed).

The primary contributions of Section 3.7 are: (1) a unified protocol that can be used for the transmission of PNs whether for refill (their reloading as the supply expires), usage within a new region under the same CA (intra-regional), or usage within a new region under a different CA (inter-regional); (2) the incorporation of control channel and service channel intervals and the multiple service channels which are uniquely available to networks under the draft IEEE 1609 standard; (3) the extension of such a protocol across multiple RSUs to provide a more scalable solution to the distribution of PNs problem; and (4) the inclusion of a control mechanism to prevent endless flooding of PNs in these subsequent RSU transmissions.

3.7.1 A Word on Privacy

Various authors have noted that privacy is not absolute in VANETs (such as Chaurasia, et al, with the “global adversary” discussed in [94]). And while we believe privacy ought to be maximized so long as security is preserved, we also believe that to demand greater privacy than what is currently afforded by vehicles without VANET capability is unreasonable. At present and without VANETs, cars can be tracked by interested parties and linked to their owners (via license plates). Thus the focus of VANETs cannot be the achievement of absolute privacy, but rather an equivalent privacy to what drivers in the world enjoy today. It is for this reason pseudonyms were introduced to provide defense against long-term tracking and eliminate the ability of an unauthorized user identifying the behavior of a vehicle by simply reviewing network logs.

3.7.2 Pseudonym Refill

Given that within a VANET security relies on the use of asymmetric cryptography and privacy depends on the relatively frequent shift in public keys, there exists a need for new keys on an ongoing basis. Refilling PN strategies are varied and extend from (a) the technologically simple but user’s time intensive approach of plugging in a vehicle to (b) the need for almost ubiquitous RSUs to provide pseudonyms at any given instant on a frequently recurring basis [65]. In the protocol presented in this section, a balance is struck to reduce the overall number of times a vehicle must refill its pseudonyms while keeping the refill almost invisible to the vehicle's driver.

3.7.3 Regions

Upon their deployment, it is assumed that VANETs will be broken up into autonomous regions [72]. Some of these regions will fall within a single CA, the crossing of which can be described as **intra**-regional. Others, however will be under different CAs and thus will require **inter**-regional certificate exchanges. The protocol we present works in both situations.

3.7.4 Pseudonym Generation

One of the important questions in the use of pseudonyms is their generation. It is possible for them to be generated by the vehicle, sent to a CA to be signed, and then sent back for vehicle use. Or they could be generated by the RSUs, signed by the CA, and then sent to the vehicles for use. Thirdly, they could be generated by a third party, signed by the CA, and then sent to the vehicle for use. Finally, the CA itself could generate them and send them to the RSU for distribution.

The first case places the burden of processing on the OBUs but reduces what needs to be transmitted to only the public keys. This has a potential security weakness in that the CA does not have a copy of the private key (which does enhance privacy) and thus is unable to confirm a valid key pair exists (it simply is signing whatever the OBU sends to it). The second case shifts the processing to an RSU, which is presumably more computationally capable than an OBU, and relieves the CA of having to do all the processing. This provides greater security in that the key pairs are being generated by the infrastructure vice the vehicle, but runs into issues if the vehicle does not stay near the RSU long enough to receive the keys being generated. Using a third party also removes the processing from the OBU and RSU but introduces an additional host into the transaction. Using a server at the CA to generate the key pairs provides the greatest security in assuring that the keys are valid and provides for central management of the key distribution. For this reason, our protocol assumes this fourth case, but could be adapted for any of the others.

A final important note regarding PN generation is the time required to perform this task. Most likely, sufficient PNs will be downloaded to vehicles to cover a certain temporal period (such as three, six, nine, or 12 months). Thus the time it takes to generate a larger set of pseudonyms is not insignificant. Ideally, the refill could be anticipated and the keys pre-generated to save this time. Regardless, the keys will still need to be transmitted from the generator to the distributor and finally to the user.

3.7.5 Single RSU Pseudonym Distribution

As mentioned in 3.7.2, one of the methods of PN distribution is on an individual basis as an OBU contacts an RSU. Concerns with this method include the need for a large density of RSUs and the frequent use of the VANET bandwidth. Previous work discussed the possession of PNs to support a longer term of usage (such a one year as in [43]). Thus one of the important questions is: how much data can a vehicle acquire during a single pass of an RSU? This is a hard question to answer as it is based upon many factors including the speed of the vehicle (and changes in speed), the distance the vehicle is from the RSU (and changes in direction), the density of other vehicles (in terms of beacons on the control channel), the VANET bandwidth utilization (in terms of throughput on the service channels), the number of channels being used, the OBU and RSU radio range, and so on.

Using ns-3 [95], we simulated a single vehicle passing a single RSU at various speeds and distances to provide some insight into the "ideal" throughput achievable. We used IEEE 802.11p to model the physical layer and IEEE 1609.4 to model the MAC layer (more details of the simulation configuration are provided in Section 4.4). Our simple protocol relied on the vehicle sending out a request message upon receipt of an RSU beacon and the RSU continuing to send PNs provided it received OBU beacons. This simulation did not take into account processing time or transmission time from the PN generator to the RSU. The simulation setup is shown in Figure 16 and the results are shown in Figure 17.

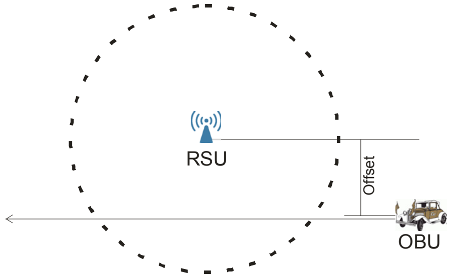


Figure 16. Simulation Topography

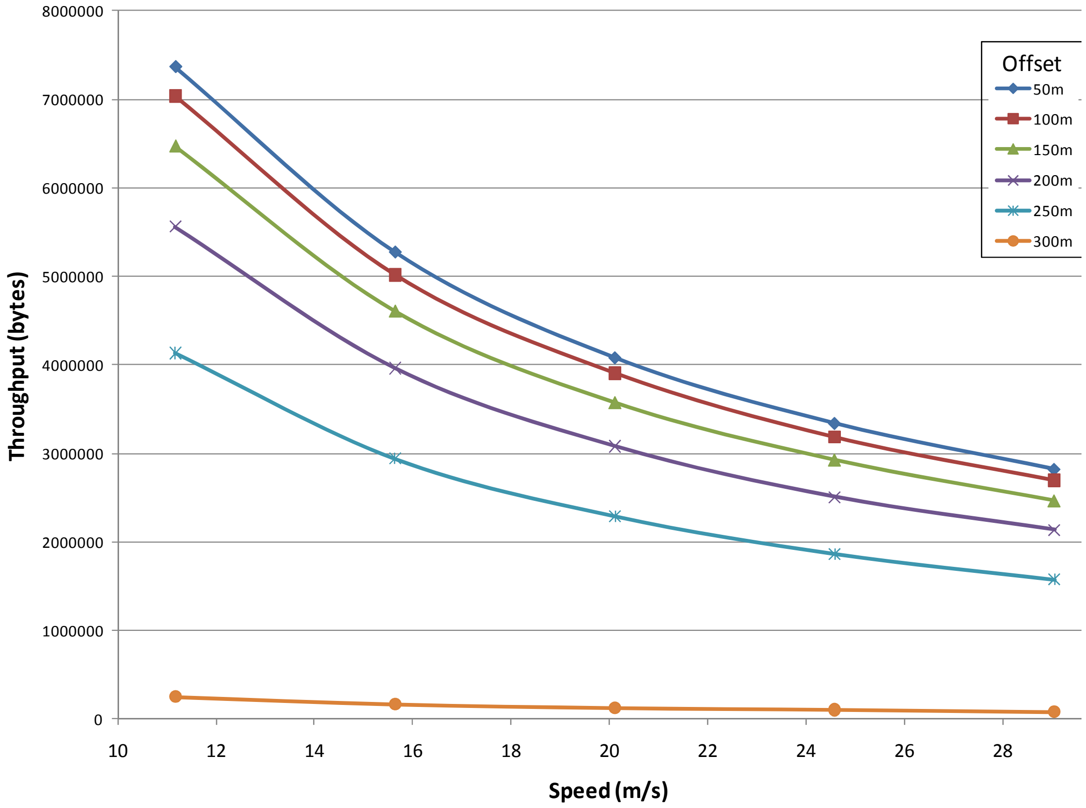


Figure 17. Plot of Simulated Throughputs

Under these "ideal" conditions and travelling at typical driving speeds, a maximum of 7.1 Megabytes were able to be received (at a speed of 11.2 meters/second (25 MPH) and 15 meters offset as defined in Figure 16). Using PN sizes from [96], this corresponds to approximately 48,686 PNs or about one year's worth using one PN per minute and having only two hours' worth of PNs per day (as was the case proposed in [72]). However, if one uses more PNs per day, shift them more frequently, drive (on average) more quickly, have other vehicles competing for the service channel, or pass further from the RSU, one will not be able to get a year's worth of PNs in a single pass.

Our protocol is introduced to facilitate the distribution of PNs within a region, intra-regionally, and inter-regionally.

3.7.6 Pseudonym Distribution Protocol (PNDP)

The ephemeral nature of VANETs provides for limited time windows for communication between vehicles and infrastructure. Thus, in order to transmit a file of greater size over a VANET, one could increase this window (by slowing the vehicle down or even making it stop). Another approach, and the one we take, is to concatenate multiple windows together in an effort to make the process invisible to the driver. The basic protocol works as follows.

When a vehicle determines more (of the same region) or new (of a different region) pseudonyms are needed, it begins to monitor the control channel (CCH) transmissions for an RSU beacon advertising PN services. Upon receiving such a beacon, it transmits in the next service channel (SCH) a request for pseudonyms. As this is the first request, the RSU will initiate pseudonym generation (using one of the methods in 3.7.4 above). As soon as PNs are available for distribution, and provided a beacon was received by that OBU in the previous CCH, the RSU will transmit the PNs to the OBU. The RSU will continue to do this as long as corresponding beacons are received in the CCH. Once a certain number of consecutive control channels pass with no such beacons being received, the RSU determines the OBU to be out of range.

Table 8. Summary of variables used in PNDP.

M_f	The maximum times the remaining PNs can be forwarded by RSUs that have not had contact with the OBU of interest
M_r	The maximum consecutive control channels that can elapse where the OBU does not receive a beacon from the current RSU before the protocol resets
M_o	The maximum consecutive control channels that can elapse where the RSU does not receive a beacon from the current OBU before the protocol resets
PNBFC	Pseudonym Block Forward Count: variable that represents the number of times the current block of PNs has been forwarded
RNBC	RSU No Beacon Count: variable that increments each time a CCH passes with no beacon received from the RSU of interest ; resets to 0 each time such beacon received by the OBU
ONBC	OBU No Beacon Count: variable that increments each time a CCH passes with no beacon received from the OBU of interest; resets to 0 each time such beacon is received by the RSU

Now begins the forwarding portion of the protocol to minimize the delay for obtaining the remaining PNs during further OBU-RSU contacts. The RSU forwards to the most likely RSU(s) (as discussed below) the remaining PNs beginning with the first PN during the last SCH where PNs were transmitted (thus the last block sent will be available for re-transmission as the OBU left the RSU's range sometime after its last OBU beacon was received/the previous PN block was acknowledged and when its next beacon should have been received).

One of the potential circumstances is that an RSU could receive a block of PNs but never encounter the OBU. To address this problem and provide a graceful conclusion to the protocol from such an RSU's perspective, we introduce two fields in the PN forward message. The first one indicates the number of times the current block of pseudonyms has been forwarded (PN Block Forward Count or PNBFC) and the second is the maximum times the block can be forwarded without an RSU contacting the OBU (M_f). Thus the RSU who has had no contact with the OBU could either drop the PNs (which would occur when $M_f = 1$, that is the block was forwarded to it, so PNBFC already is one) or forward them on to the next adjacent RSU(s) (which would occur when

$M_f > 1$). Another feature of this field is to forbid additional RSUs from forwarding PNs at all by setting M_f to zero. (These variables are best implemented through a single "count down" variable which is initially set to M_f, when this variable reaches zero, no more forwarding is performed. A list of variables used in PNDP is provided in Table 8).

Meanwhile, the OBU continues to determine if it still needs PNs and if not, the protocol ends. If it does, it again monitors its CCH for RSU beacons. Upon receiving one, it sends a PN request message during the next SCH indicating the next PN it expects to receive. Upon receiving this message, the RSU should already have the PNs and be able to begin transmitting.

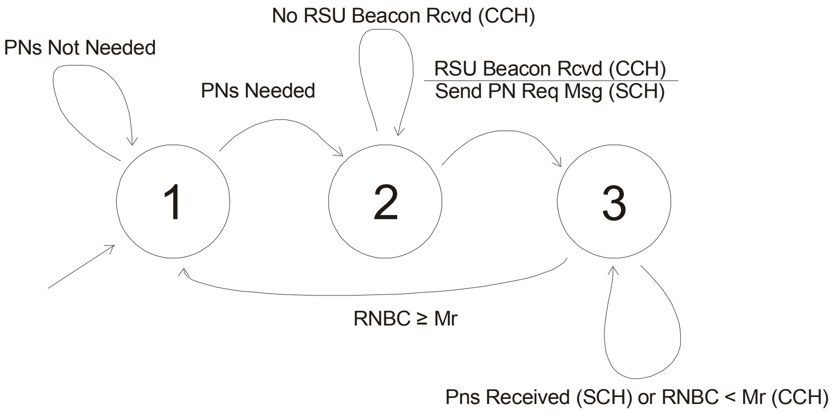


Figure 18. PNDP state diagram (OBU).

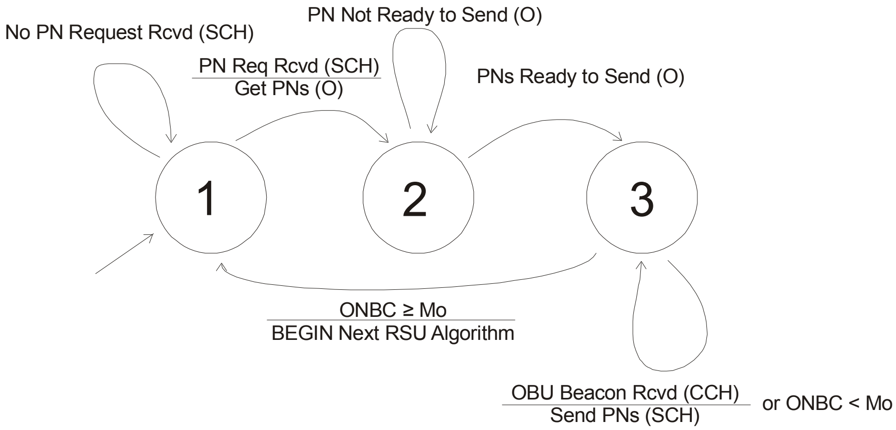


Figure 19. PNDP state diagram (RSU).

The previously described steps continue until all the PNs have been distributed. Figure 18 and Figure 19 illustrate the state diagrams for the OBU and RSU respectively. M_r represents the maximum consecutive CCH intervals for the OBU to experience with no RSU beacon being received before determining the RSU is out of range. M_o fulfills the same purpose for the RSU with regards to the OBU. RNBC is the "RSU No Beacon Count" which is incremented each time a CCH interval passes with no beacon received from the RSU of interest and reset to 0 each time such a beacon is received by the OBU. ONBC performs the same function for the RSU.

The protocol diagram for PNDP is provided in Figure 20 and provides more detail regarding the content of the messages being exchanged. The vehicle makes the initial request for additional PNs using its long term key and its current PN (1). This authenticates both the vehicle and the validity of the current PN which are then verified to be linked by the CA. The RSU responds with a symmetric key encrypted with the vehicles public key and signed by the CA as well as the service channel to use for the duration of the transmissions (2). This service channel can be changed during any subsequent control channels. The vehicle in (3) then makes a PN block request by sending its PN and the key encrypted using the CA's public key. This exchange is repeated for all future requests so that the RSU can validate the user and ensure it is using the correct symmetric key. The RSU responds by sending as many PNs as possible during each service channel where it receives an OBU beacon in the previous control channel (or at least one in the previous M_o control channels) (4). When the no-beacon counts (RNBC and ONBC) time out, the OBU and RSU determine themselves to be out of range (7) and the RSU forwards the remaining block of PNs to the next most likely

RSU(s). In (8), the OBU has received a beacon from the next RSU and again makes a PN request. In this request it sends its current PN as well as two pieces of information encrypted by the symmetric key: its previously used PN to link the transaction and the next expected PN block.

3.7.7 Pseudonym Blocks

The actual transmission of PNs would be performed in “blocks” (of 8 for example) based upon the MTU and the size of the certificates. IEEE 1609.2 specifies each PN to be 153 bytes [26] while the addition of a “valid from” field (which we advocate) would increase this size to 157 bytes [96]. Each of these blocks would be numbered to facilitate the next RSU transmitting at the next needed block with minimal retransmissions. The total number of blocks is transmitted in step two of the protocol so the OBU knows when the total intended transmission is complete. Should the OBU leave the RF range of all RSUs prior to receiving the total number of blocks, it will know more are needed upon its return (or could notify the driver).

3.7.8 Modified Diffie-Helman

In order to protect the secrecy of the PNs and provide greater efficiency (quicker decryption), their transmission would be encrypted using a symmetric algorithm, such as AES. During the initial request for PNs, the OBU would send its signed long-term key (as discussed in [69]) along with its current public key (represented by $CA^{-}(V^{+})$, i.e. the CA signed public key of the OBU) which would allow the CA to link this vehicle to all its pseudonyms it will use during the transmission. The RSU will respond with the symmetric key which it has signed and, using the vehicle’s public key, encrypted. The

OBU will then request PNs by sending its current pseudonym and the next expected block number encrypted using the now shared key. The RSU responds with the OBU's current PN signed (so that other vehicles can quickly discard the packet) and as many blocks of PNs (signed using the symmetric key) it can transmit in the service channel. This layer of abstraction is illustrated in Figure 20 with the abbreviations used listed in Table 9.

Table 9. Protocol diagram abbreviations.

V+	Current Vehicle Public Key
V-	Current Vehicle Private Key
CA+	Regional Certificate Authority Public Key
CA-	Regional Certificate Authority Private Key
CA-(V+)	A Pseudonym (the CA signed public key)
KEY	Symmetric Shared Key
$PN_{\#}$	Total # of PN blocks the CA intends to send
TPNB	Block of Numbered and Sequential Psedonyms
VIN#	Unique Vehicle Identification Number
prev()	Previous Operator (used to link transaction)
x	PN window size (# that can be sent in 46 ms)
y	Last in-order received PN

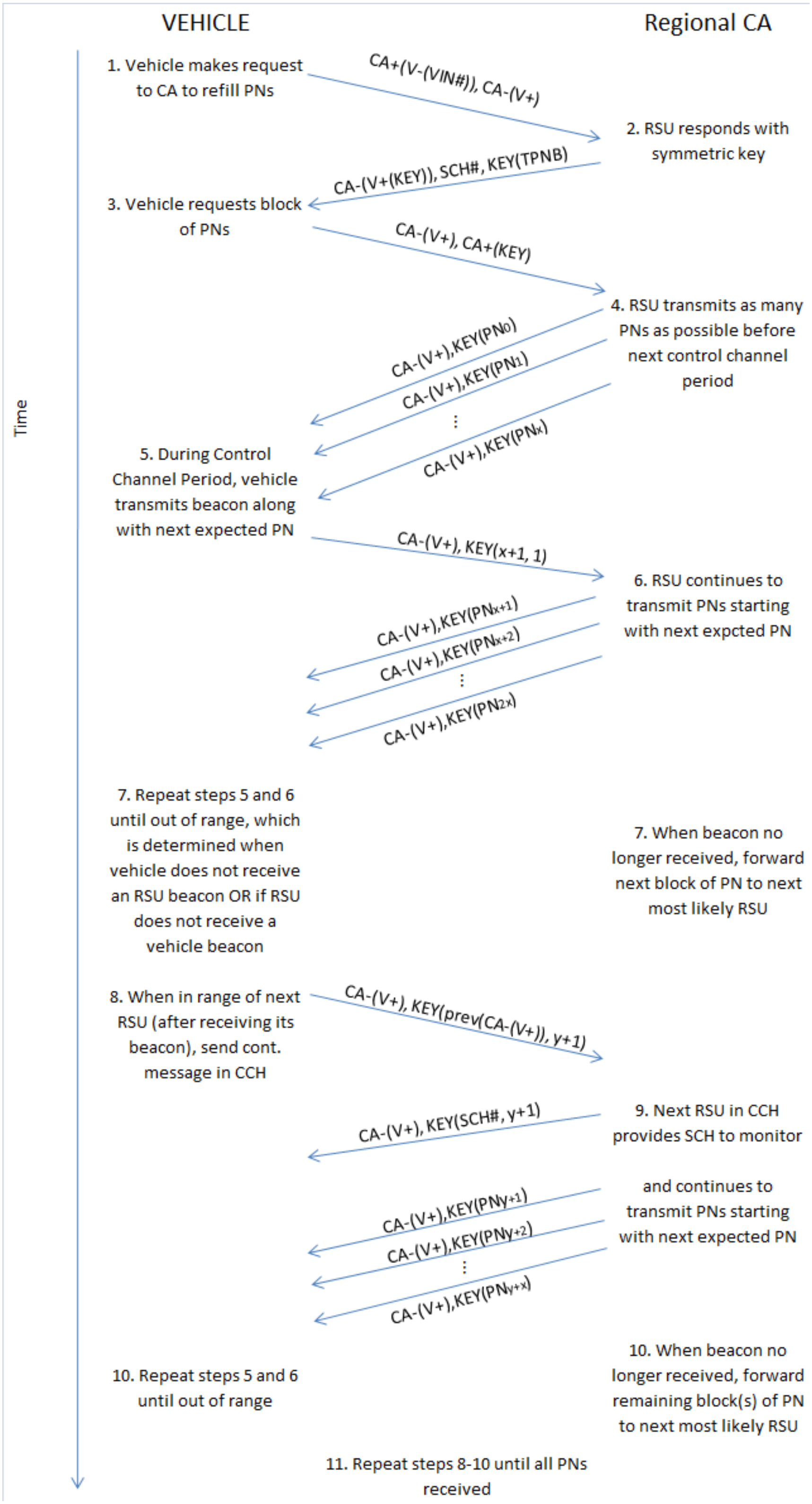

VEHICLE
Regional CA
Time
1. Vehicle makes request to CA to refill PNs
CA+(V-(VIN#)), CA-(V+)
2. RSU responds with symmetric key
CA-(V+(KEY)), SCH#, KEY(TPNB)
3. Vehicle requests block of PNs
CA-(V+), CA+(KEY)
4. RSU transmits as many PNs as possible before next control channel period
CA-(V+),KEY(PN$_0$)
CA-(V+),KEY(PN$_1$)
⋮
CA-(V+),KEY(PN$_x$)
5. During Control Channel Period, vehicle transmits beacon along with next expected PN
CA-(V+), KEY(x+1, 1)
6. RSU continues to transmit PNs starting with next expcted PN
CA-(V+),KEY(PN$_{x+1}$)
CA-(V+),KEY(PN$_{x+2}$)
⋮
CA-(V+),KEY(PN$_{2x}$)
7. Repeat steps 5 and 6 until out of range, which is determined when vehicle does not receive an RSU beacon OR if RSU does not receive a vehicle beacon
7. When beacon no longer received, forward next block of PN to next most likely RSU
8. When in range of next RSU (after receiving its beacon), send cont. message in CCH
CA-(V+), KEY(prev(CA-(V+)), y+1)
9. Next RSU in CCH provides SCH to monitor
CA-(V+), KEY(SCH#, y+1)
and continues to transmit PNs starting with next expected PN
CA-(V+),KEY(PN$_{y+1}$)
CA-(V+),KEY(PN$_{y+2}$)
⋮
CA-(V+),KEY(PN$_{y+x}$)
10. Repeat steps 5 and 6 until out of range
10. When beacon no longer received, forward remaining block(s) of PN to next most likely RSU
11. Repeat steps 8-10 until all PNs received

Figure 20. Protocol Diagram

3.7.9 Next Most Likely RSU

The next most likely RSU can be determined a number of ways. In the worst case scenario it is inaccurately determined and the RSU the OBU contacts will have no prior knowledge of its need for PNs. The RSU will have to contact the CA thus replicating the overhead of the initial RSU. It is our goal to avoid this situation; however if it does occur we are no worse off than not having a multiple RSU protocol to transmit PNs.

A slightly better approach would be to send the remaining blocks of PNs to the next RSU the vehicle would encounter based upon its current trajectory. Then if the OBU encounters this RSU next, the PNs are preloaded and transmission can begin almost immediately. However the vehicle is apt to make turns in which case it may never encounter this RSU.

A different approach is to flood all adjacent RSUs with the information as the vehicle will most likely come in contact with one of these next. This is a reasonable solution given that the out-of-VANET-band network (i.e. the infrastructure-to-infrastructure or I2I network) is used and maximizes the likelihood that the OBU will contact an RSU that has been pre-loaded with its PNs. It is worth noting that this still does not guarantee the vehicle will cross paths with an RSU that has been preloaded as the vehicle could pass between two RSUs in a dead zone that neither has coverage (or it could stop short between the past RSUs and any other ones).

Finally, with the growing use of navigational systems in cars, it is believed that in-dash as well as external units could be utilized to provide routing information to the OBU. Using this information, the OBU could optionally provide its path to the CA which would then pre-load the PNs on the RSUs along that path.

3.7.10 Multi-Channel Usage

One of the unique features of VANETs is the six service channels provided for in the draft standards IEEE 1609.4 [97]. Our protocol takes advantage of this to either transmit PNs to more than one vehicle or leave other channels open for other applications.

3.7.11 Inter-Regional Certificate Authorities

In [69] we discussed a methodology for regions and PN usage. This protocol builds upon this (or could be adapted to other approaches) by providing a protocol to transmit the PNs to the OBUs. In cases where vehicles are transiting beyond regions covered by a single root CA, the OBU will also need additional public keys of the various regions covered by the new CA. Thus at inter-regional crossings, the RSU must be prepared to also transmit, prior to the PNs, these public keys. Such RSUs would expect this and have the keys readily available.

Probably less obvious is the need for RSUs at borders to verify the validity of the presently valid PNs that have been issued by a different CA. Of course the RSUs will have ready access to such keys given they will have a networked connection to the Internet (unlike OBUs), however policies must be in place to accept such PNs and permit the issuance of locally generated PNs by the inter-regional entity to the “foreign” OBU.

3.7.12 Scalability of PNDP

As the density of VANET enabled vehicles increases, the need for a protocol that can span multiple RSUs becomes even more important. OBUs will have a hard time monopolizing the bandwidth of a single RSU while within range of each other.

Scalability is one of the greatest features of this protocol as it allows for larger numbers of OBUs to participate among the available RSUs by taking advantage of the multiple channels provided.

3.7.13 PNDP Conclusion

The use of pseudonyms is a critical component to preserving privacy while permitting authentication in VANETs. Much work has been accomplished in fine tuning the details of this arrangement. This work has demonstrated through simulated results that a single pass of an RSU is insufficient to provide the bandwidth necessary for an OBU to acquire sufficient PNs for longer terms of usage. We have presented a unified protocol for the dissemination of such PNs for refill as well as the crossing of both intra-regional and inter-regional borders that provides scalability while taking advantage of the unique characteristics of VANETs. The next step is to validate these ideas via the use of realistic simulations.

CHAPTER 4

SIMULATION METHODOLOGY

4

4.1 Introduction

Few tools, if any, have ignited the technological revolution that we experience today more than simulation. Simulation has been defined as the "process of building and analyzing the output of computer programs that describe the operations of an organization, process, or physical system" [98]. Engineers and scientists have used simulation to design, improve, or increase understanding of many facets of society. Electrical engineers use simulation in such diverse endeavors as controls, circuits, power, electromagnetics, and telecommunications to name a few. Simulation allows for rapid prototyping, reduced expenses, and valuable knowledge and experience. Thus simulation is a natural choice to assess various qualities of pseudonym distribution. While simulation is this powerful tool, we are also reminded that it is the "imitation of the operation of a real-world process or system over time" and as such has limitations [99]. It is important to document the environment in which a simulation takes place so that it is repeatable and its results can be clearly understood from within these parameters. This section seeks to do just that.

4.2 Network Simulator 3 (ns-3)

The Network Simulator was first conceived in 1989 as the REAL network simulator [100]. From 1995-1996 a discrete-event network simulator, called ns-1, was developed at Lawrence Berkeley National Laboratory, a national Department of energy lab using C++ with Tcl script based simulations [101]. From 1996 to 1997, its successor ns-2 was developed (originally by Steve McCanne) in C++ with an object-oriented scripting language used to run simulations and ultimately improved by the legitimacy and funding of the Defense Advanced Research Projects Agency (DARPA) and later the National Science Foundation (NSF) [102]. Meanwhile at the Georgia Institute of Technology a more powerful network simulation tool known as GTNetS (for GA Tech Network Simulator) was developed completely in C++ and able to handle a previously unattainable complexity of over a million network elements [103]. In 2006, development of ns-2's replacement, ns-3, was begun as an evolution of GTNetS and partially through a grant from the NSF with large contributions from the French National Institute for Research in Computer Science and Control's Matthew Lacage. Its two co-principal investigators are Tom Henderson (Boeing/UW) and George Riley (of our own Georgia Institute of Technology) [103]. It is presently in its 15th stable release (ns-3.15) and is freely available under the GNU license [104].

4.3 Assumptions

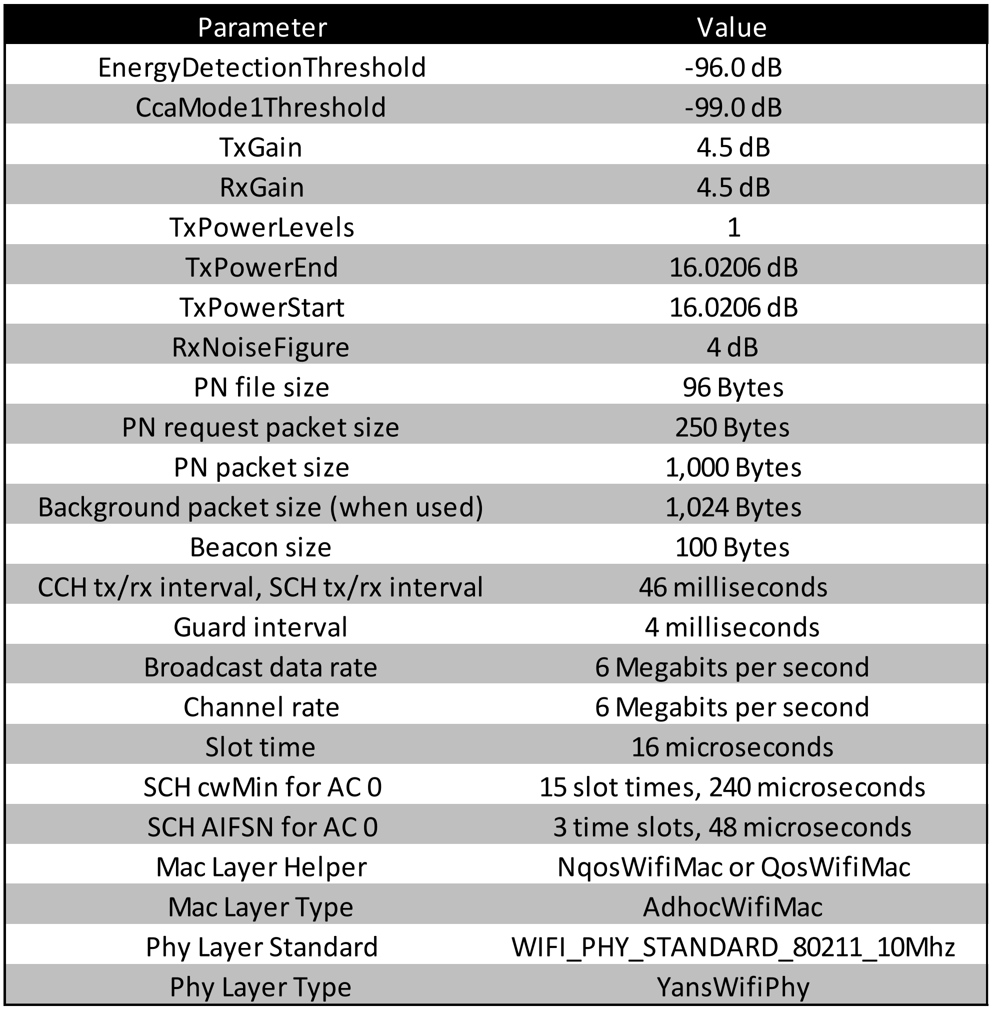
The assumptions that we made were consistent with previous research conducted by the Network Security Architecture lab at the Georgia Institute of Technology [105]. The behavior of the nodes was predicated on their function. RSU's were assumed to be stationary and placed as depicted in each simulation topography that will be provided and was designed to provide meaningful results. OBU's were either directly involved in PN distribution consistent with the goals of the experiment (for example, when examining the effect of various OBUs of various PN fills requesting PNs, when a threshold was set those OBUs involved in PN refill respected these thresholds). In some scenarios we examined the impact of PN distribution on background data transmission. In these, the background OBUs did not participate in the PN refill process and were assumed to have sufficient PNs to participate in the VANET.

Given that IEEE 1609.3 requires that all VANET nodes be compatible with OBUs that possess only a single transmitter/receiver, we focused on this scenario and did not examine multi-channel PN distribution for a given OBU. We believe this is justified due to the economy of scale involved and, while we recognize that RSUs have multiple channels, the unlikely fact that an RSU would reserve multiple of them for PN distribution in the face of other competing services. When background data was part of a scenario, it was transmitted on a separate channel from PN distribution but was given background priority over the RSU processing PN requests.

4.4 Simulation Configuration Parameters

This research involved various channel model and mobility models that are described in the following two sections and identified with each scenario in Section 5. Settings that were the same across all simulation scenarios are provided in Table 10. Other settings, such as simulation time, vehicle velocity, and transmission range are situation dependent and also individually provided in Section 5.

Table 10. Simulation configuration parameters.

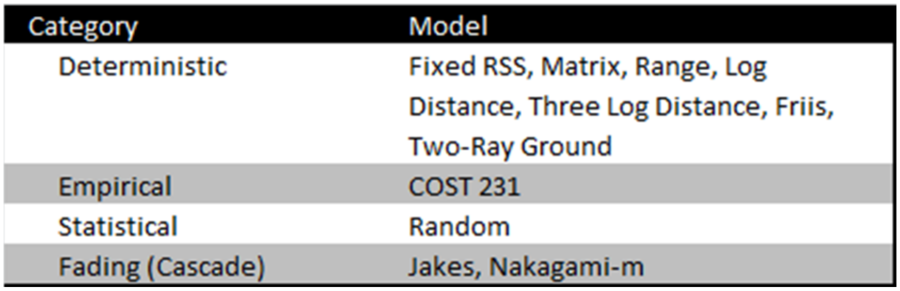


Parameter	Value
EnergyDetectionThreshold	-96.0 dB
CcaMode1Threshold	-99.0 dB
TxGain	4.5 dB
RxGain	4.5 dB
TxPowerLevels	1
TxPowerEnd	16.0206 dB
TxPowerStart	16.0206 dB
RxNoiseFigure	4 dB
PN file size	96 Bytes
PN request packet size	250 Bytes
PN packet size	1,000 Bytes
Background packet size (when used)	1,024 Bytes
Beacon size	100 Bytes
CCH tx/rx interval, SCH tx/rx interval	46 milliseconds
Guard interval	4 milliseconds
Broadcast data rate	6 Megabits per second
Channel rate	6 Megabits per second
Slot time	16 microseconds
SCH cwMin for AC 0	15 slot times, 240 microseconds
SCH AIFSN for AC 0	3 time slots, 48 microseconds
Mac Layer Helper	NqosWifiMac or QosWifiMac
Mac Layer Type	AdhocWifiMac
Phy Layer Standard	WIFI_PHY_STANDARD_80211_10Mhz
Phy Layer Type	YansWifiPhy

4.5 Simulation Channel Loss Models [106]

Given its tremendous impact on the validity of the results, extensive research was conducted into the channel loss models supported by ns-3 in order to provide the most realistic propagation scenario for these simulations. A large variety of propagation loss models are available for use. The network simulator 3 release 10 (ns-3.10) natively supports eleven different such models, listed in Table 11, and discussed in the subsequent subsections. The propagation loss models can be categorized as deterministic, empirical, or statistical, and ns-3 provides at least one of each. Furthermore, ns-3 also provides the ability to cascade models, including the addition of the probabilistic Nakagami fast fading model.

Table 11. Native propagation loss models of ns-3.10

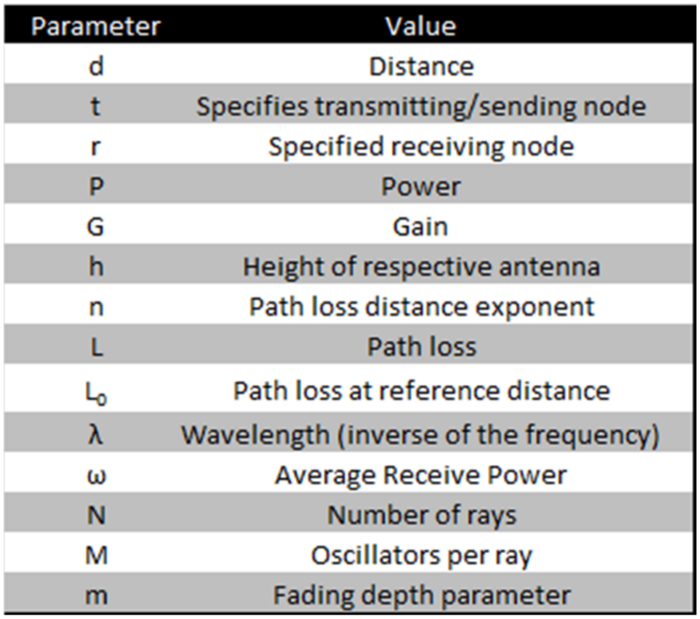


Category	Model
Deterministic	Fixed RSS, Matrix, Range, Log Distance, Three Log Distance, Friis, Two-Ray Ground
Empirical	COST 231
Statistical	Random
Fading (Cascade)	Jakes, Nakagami-m

Table 12 lists the variables used in our work. In general, simulators use a defined minimum receive power as the threshold to determine if a packet can be successfully received. The simulated receive power (enumerated in Equation 4) is compared to this minimum required receive power and either the packet is received or "lost." For 802.11p simulated in ns-3, the default transmit power (`TxPowerStart` and `TxPowerEnd`) is 16.0206 dB and the `EnergyDetectionThreshold` is -96 dB, which represents the minimum receive power for the receiver. Thus a loss of 112.0206 dB renders a packet "lost" in ns-3 [107].

$$P_r = P_t - L \tag{4}$$

Table 12. Model loss variables used



Parameter	Value
d	Distance
t	Specifies transmitting/sending node
r	Specified receiving node
P	Power
G	Gain
h	Height of respective antenna
n	Path loss distance exponent
L	Path loss
L_0	Path loss at reference distance
λ	Wavelength (inverse of the frequency)
ω	Average Receive Power
N	Number of rays
M	Oscillators per ray
m	Fading depth parameter

4.5.1 Non-Applicable Models to VANETs [108]

When modeling the VANET environment, some of the offered models within ns-3 simply do not apply. The `FixedRssLossModel` for example yields a constant received power regardless of the distance between sender and receiver. The `MatrixPropagationLossModel` is equally unusable for VANET modeling as it fixes the propagation loss for each pair of nodes regardless of their actual positions. Finally, the `RandomPropagationLossModel` is also a poor choice as it simply selects a value each time a packet is received following a user defined random distribution. Finally, the `RangePropagationLossModel` uses the transmit power as the received power for distances between sender and receiver less than or equal to the specified "range" and a received power of -1000 dBm beyond this distance.

4.5.2 Non-Applicable Empirical Model [108]

From April 1989 until April 1996, the European Union sponsored the COperation européenne dans le domaine de la recherche Scientifique et Technique (COST) forum that produced the COST 231 propagation loss model for use in dense locations (both indoors in the midst of a many-walled office or outdoors in dense urban environments) [109]. As an empirical model, it uses previously collected data as its basis and thus is very fast but generally less accurate for a given scenario. Furthermore, this model was only designed for use in 1.5 to 2 GHz frequency range and as such is not a good choice to model VANET propagation loss.

4.5.3 Basic Models [108]

Four basic propagation loss models, all deterministic in nature, are provided for in ns-3.10: Log Distance, Three Log Distance, Friis, and Two-Ray Ground.

The `LogDistancePropagationLossModel` and the `ThreeLogDistancePropagationLossModel` incorporate the same calculation for propagation loss except that the three log model provides for four distance fields. Equation 5 is known as the log distance equation while Equation 6 provides the complete three log distance equation. The log distance model provides for basic attenuation and is normally associated with indoor environments, such as for use with wireless LANs. It is worth noting that it is the default propagation model of the YANS physical layer helper class in ns-3.10. The three log-distance model provides for additional tuning but is generally seen as an indoor or urban propagation loss model.

$$L = \begin{cases} 0 & \mathrm{d} < \mathrm{d}_0 \\ L_0 + 10 \cdot n_0 \log_{10}\left(\frac{d}{d_0}\right) & \mathrm{d} \geq \mathrm{d}_0 \end{cases} \tag{5}$$

$$L = \begin{cases} 0, & d<d_0 \\ L_0+10\cdot n_0 \log_{10}\left(\frac{d}{d_0}\right), & d_0\leq d<d_1 \\ L_0+10\cdot n_0 \log_{10}\left(\frac{d_1}{d_0}\right)+10\cdot n_1 \log_{10}\left(\frac{d}{d_1}\right), & d_1\leq d<d_2 \\ L_0+10\cdot n_0 \log_{10}\left(\frac{d_1}{d_0}\right)+10\cdot n_1 \log_{10}\left(\frac{d_2}{d_1}\right)+10\cdot n_2 \log_{10}\left(\frac{d}{d_2}\right), & d_2\leq d \end{cases} \tag{6}$$

The `FriisPropagationLossModel`, is a simplified version of the log distance propagation loss model. Rather than using loss coefficients that must be empirically acquired and validated, it simplifies the propagation loss calculation to that given in Equation 7. It is not accurate for very small distances (the default minimum distance in ns-3.10 is .5 meters).

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi d)^2 L_0} \tag{7}$$

The `TwoRayGroundPropagationLossModel` considers both the direct path and a ground reflection path when calculating the received power in accordance with Equation 8. This model is often viewed as an accurate selection when modeling rural environments [110]. Thus for research in strictly rural environments, this simple propagation loss model may be of use.

$$P_r(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4} \tag{8}$$

4.5.4 Accounting for Fading in ns-3 [108]

It is possible in ns-3 to account for fading when using the propagation loss models discussed in Section 4.5 by applying either the Jakes or Nakagami models (to be implemented normally in addition to a propagation loss model).

The `JakesPropagationLossModel` implements a modified Jakes model (concisely presented in [111]) which seeks to incorporate Rayleigh fading and simplify its calculation. It uses a set of electromagnetic rays that would depart the transmitter in order to determine which ones would reach the receiver. These sinusoidal rays are then summed to determine the received power level. Jakes propagation loss is defined by Equations 96 and 10 [111]. It is worth noting that the initial phase shifts (ϕ) can be randomly generated according to a specified distribution, which however by default is a constant in ns-3.10. This fading model is most appropriate where multi-path is a significant issue and no line of sight exists between the sender and receiver, which is often the case in urban (or indoor) environments.

$$X(t) = \mathrm{X_c(t) + jX_s(t)} \tag{9a}$$

$$X_c(t) = \frac{2}{\sqrt{\mathrm{M}}} \sum_{\mathrm{n=1}}^{\mathrm{M}} \cos(\psi_\mathrm{n}) \cdot \cos(\omega_\mathrm{d} \mathrm{t} \cos \alpha_\mathrm{n} + \phi) \tag{9b}$$

$$X_s(t) = \frac{2}{\sqrt{\mathrm{M}}} \sum_{\mathrm{n=1}}^{\mathrm{M}} \sin\,(\psi_\mathrm{n}) \cdot \cos(\omega_\mathrm{d} \mathrm{t} \cos \alpha_\mathrm{n} + \phi) \tag{9c}$$

$$\alpha_n = \frac{2\pi n - \pi + \theta}{4M}, n = 1, 2, \ldots, M \tag{10}$$

The `NakagamiPropagationLossModel` applies the Nakagami fast fading distribution to the received power level and serves to transform otherwise deterministic propagation loss models to probabilistic ones. The Nakagami probability density function is defined in Equation 11 and, similar to the three log-distance model, is defined over three distance fields (0 to d_1 is m_0, d_1 to d_2 is m_1, and d_2 to d_3 is m_2). When m equals one, the Nakagami distribution equals the Rayleigh distribution.

$$p(x; m, \omega) = \frac{2m^m}{\Gamma(m)\omega^m} x^{2m-1} e^{-\frac{m}{\omega}x^2} \tag{11a}$$

$$= 2x \cdot p_{Gamma}\left(x^2, m, \frac{m}{\omega}\right) \tag{11b}$$

4.5.5 Propagation Loss Model Summary

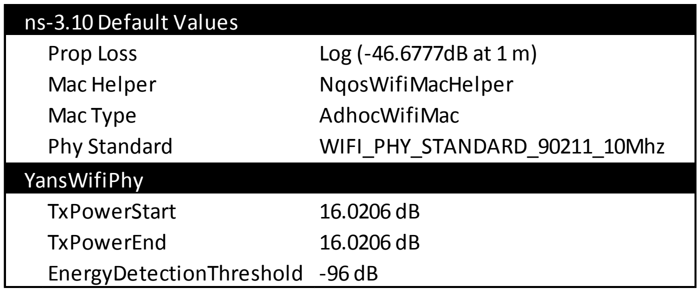
The preceding paragraphs demonstrate that ns-3 provides those who desire to simulate vehicular networks three propagation loss models geared for urban environments, one for rural environments, and the ability to make these more realistic by adding Nakagami-m or Jakes fading.

4.6 Identifying Simulation Values for a Realistic Communications Range

The exact range of VANET communications is difficult to determine. Such factors as terrain, vegetation, and buildings, as well as RF interference from other transmitters in the 5.9 GHz spectrum have direct impact. Furthermore, policy and standards serve to limit the effective range to maximize the number of supportable users. The literature reflects a maximum range of 300 m for VANETs [112-114] which is consistent with experimental measurements of dedicated short range communications (DSRC) performed to date [115-117]. In these studies, it is noted that communications in urban environments normally involve a range of approximately 140 meters while those in non-urban environments achieve a range of approximately 300 m. It is for this reason that we set out to produce two sets of propagation loss parameters to support simulation in each of these environments.

4.6.1 Ns-3.10 Default Propagation Loss Values

Table 13. Default simulation parameters for Section 4.6.



ns-3.10 Default Values	
Prop Loss	Log (-46.6777dB at 1 m)
Mac Helper	NqosWifiMacHelper
Mac Type	AdhocWifiMac
Phy Standard	WIFI_PHY_STANDARD_90211_10Mhz
YansWifiPhy	
TxPowerStart	16.0206 dB
TxPowerEnd	16.0206 dB
EnergyDetectionThreshold	-96 dB

Using the default values of ns-3.10 (based on MAC and PHY layer parameters specified in Table 13, which except for propagation loss reflect those of Table 10) yields a maximum range of 151.5 meters over ten simulation runs (which provides a 95% confidence interval (CI) of being within ± 2% of the maximum range). These results are shown in Figure 21. As can be seen, this is a simplistic view of propagation loss with an almost infinite slope at the maximum range. In addition, this range exceeds (albeit it by only 11.5 m) the measured 140 meter maximum of urban environments and does not reflect the 300 m measured range for non-urban environments [115-117]. Given these differences from the expected communications range in VANETs, this motivated us to perform some simulation based research to find appropriate loss parameters that researchers can uniformly use which we published in [106].

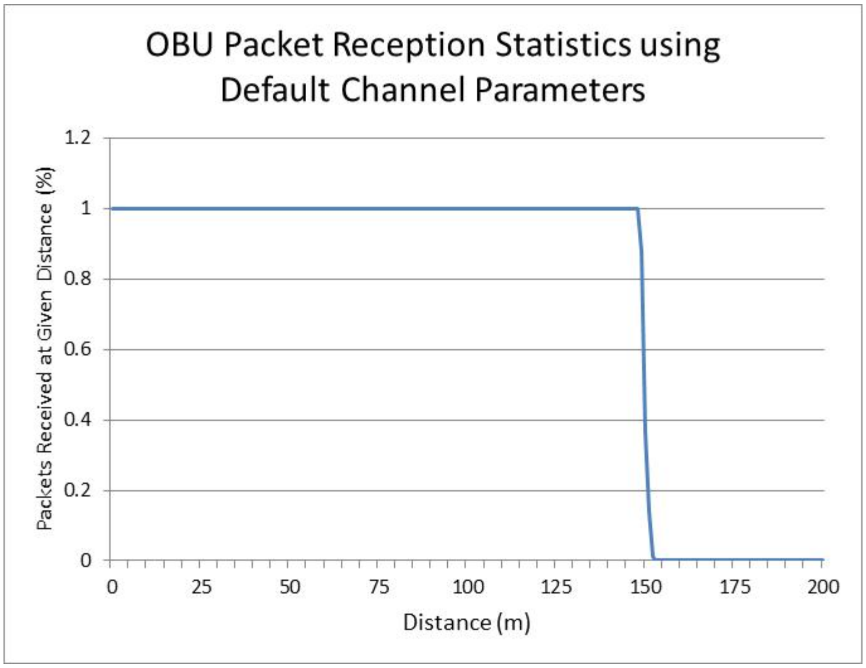


Figure 21. Default value range in ns-3.10

4.6.2 Proposed VANET Propagation Loss Parameters

This section outlines the proposed parameters for researchers to use when simulating VANETs in ns-3. All values were derived by us following the methods outlined in [99] in order to obtain a 95% CI with a half-width of 2% of the mean simulated value.

The proposed ns-3 propagation loss model parameters are summarized in Table 14 for both urban and rural simulation environments. Recall that the Two Ray Ground model has been identified as the most realistic propagation loss model for use in simulating rural environments with fewer obstructions while the log distance, three log distance, and Friis are more appropriate for urban environments.

Table 14. Summary of proposed propagation loss model parameters.

U/R	Prop Loss Model	Parameter	Value	Units	
Both	Two Ray Ground	Lambda	0.05093	meters	
Urban	Two Ray Ground	MinDistance	140	meters	
Rural	Two Ray Ground	MinDistance	300	meters	
Urban	Log Distance	ReferenceLos	37.35	dB	
Rural	Log Distance	ReferenceLos	47.2	dB	
Urban	Three Log Distance	Distance0	1	meters	*
Urban	Three Log Distance	Exponent0	2.5	unitless	
Urban	Three Log Distance	Distance1	75	meters	
Urban	Three Log Distance	Exponent1	5	unitless	
Urban	Three Log Distance	Distance2	114	meters	
Urban	Three Log Distance	Exponent2	10	unitless	
Rural	Three Log Distance	Distance0	1	meters	*
Rural	Three Log Distance	Exponent0	1.9	unitless	*
Rural	Three Log Distance	Distance1	210	meters	
Rural	Three Log Distance	Exponent1	15	unitless	
Rural	Three Log Distance	Distance2	286	meters	
Rural	Three Log Distance	Exponent2	3.65	unitless	
Both	Friis	Lambda	0.05093	meters	
Urban	Friis	SystemLoss	26.7	unitless	
Rural	Friis	SystemLoss	122	unitless	

**indicates a default value*

Adding fading is considered an important means to make a simulation of propagation more realistic. The Jakes fading model is parameter-less, while the proposed parameter values for the Nakagami-m model are listed in Table 15 for both urban and rural environments.

Table 15. Summary of proposed fading model parameters.

U/R	Fading Model	Parameter	Value	Units	
Both	Jakes	None			*
Urban	Nakagami-m	m0	1.5	unitless	*
Urban	Nakagami-m	Distance1	60	meters	
Urban	Nakagami-m	m1	0.75	unitless	*
Urban	Nakagami-m	Distance2	145	meters	
Urban	Nakagami-m	m2	0	unitless	
Rural	Nakagami-m	m0	1.5	unitless	*
Rural	Nakagami-m	Distance1	80	meters	*
Rural	Nakagami-m	m1	0.75	unitless	*
Rural	Nakagami-m	Distance2	320	meters	
Rural	Nakagami-m	m2	0	unitless	

**indicates a default value*

4.6.3 NS-3.10 Simulation Setup and Results

Two metrics were used to measure the effectiveness of the parameters proposed in Section 4.6.2. Each second a hundred packets were sent from a stationary RSU to a moving OBU traveling away from the RSU at a speed of one meter per second. The first metric was the greatest distance at which all 100 packets were received and was entitled the “effective range” (and labeled “Max 100% Dist” in the figures). The second metric was the maximum distance at which any packet was received and was primarily used to ensure consistency of the results (labeled in “Max Distance” in the figures). The aim of this work was to identify which propagation loss parameters would result in an effective range of 140 m (for urban) and 300 m (for rural) while running the necessary simulations to demonstrate the 95% CI of being within 2% of the mean.

Our results demonstrate an acquired effective range in an urban environment of 140.3, 139.9, 140.1, and 139.9 meters for the log distance, three log distance, Friis, and two ray ground models respectively and 299.5, 299.9, 299.5, and 299.9 meters respectively in a rural environment. These results are shown in Figure 22 and Figure 23, with the error bars indicating the 95% CI of the mean effective distance.

Furthermore, the maximum distance achieved reflects the nature of the probability loss models. As an example, the maximum distance of the log distance propagation loss model is a few meters greater than the three log distance model that uses progressively greater loss coefficients. Given that the two ground ray model uses a deterministic cut-off of received signal power, it stands to reason that the range of 100% reception and the maximum range be almost identical.

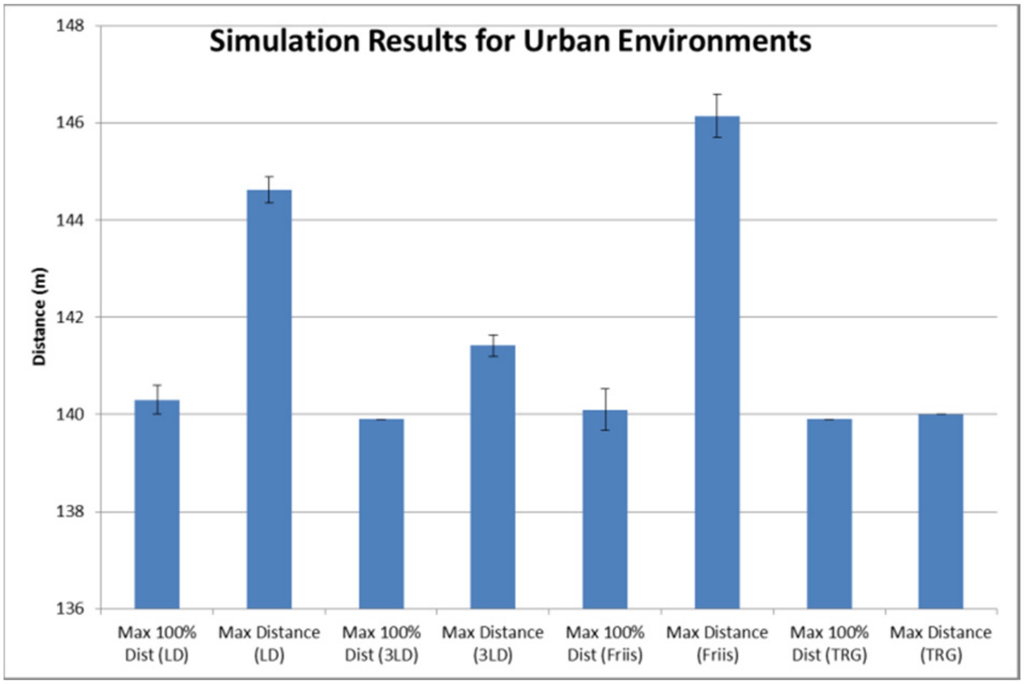


Figure 22. Propagation loss simulation results (urban)

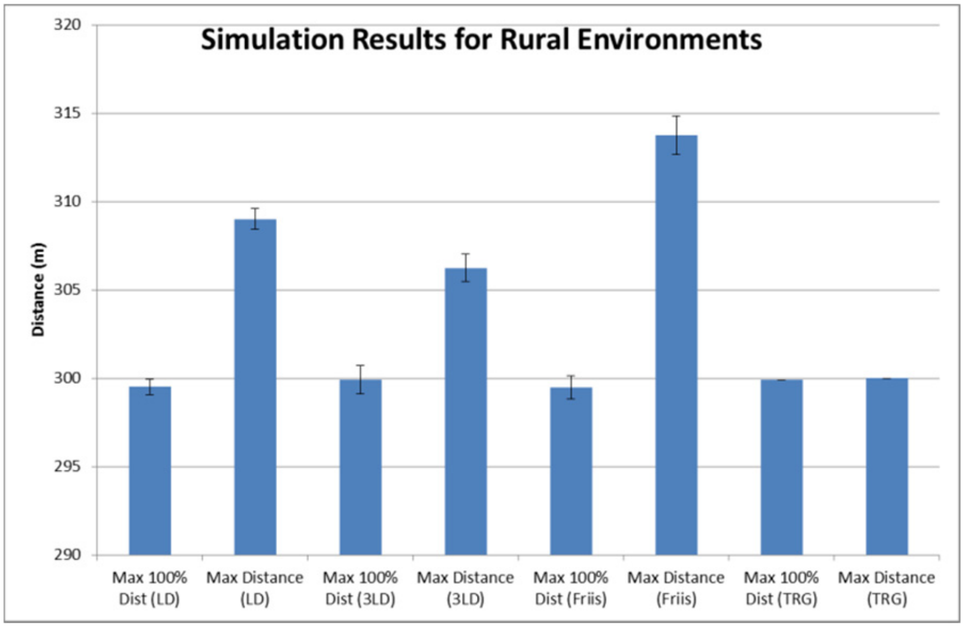


Figure 23. Propagation loss simulation results (rural)

Fading was added to a selection of propagation loss models to demonstrate their impact. These results are shown in Figure 24. To illustrate the difference between simulating packet transmissions without and with fading, a scenarios of log distance propagation loss without and then with Nakagami-m fading was simulated, the results of which are illustrated in Figure 25 and Figure 26.

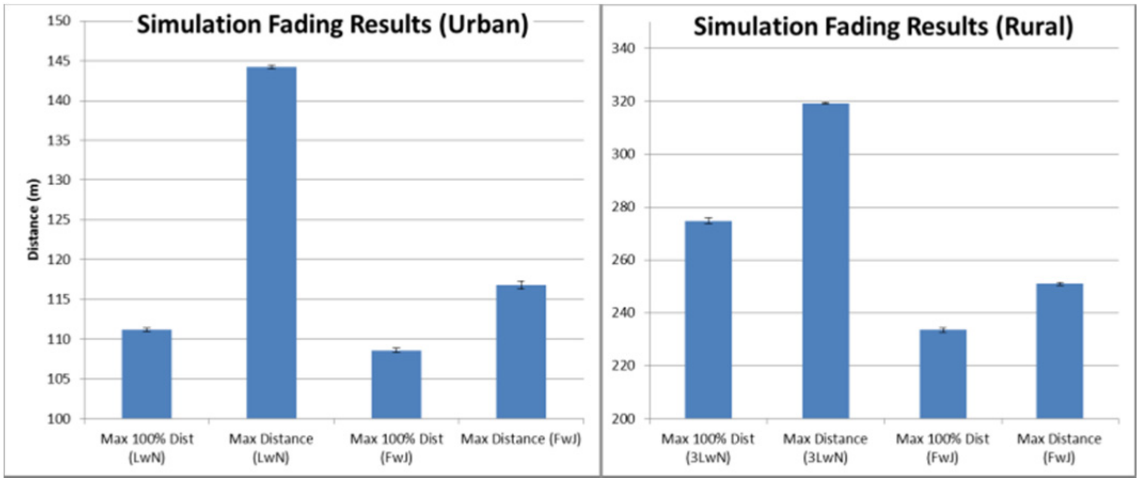


Figure 24. Fading simulation results (urban)

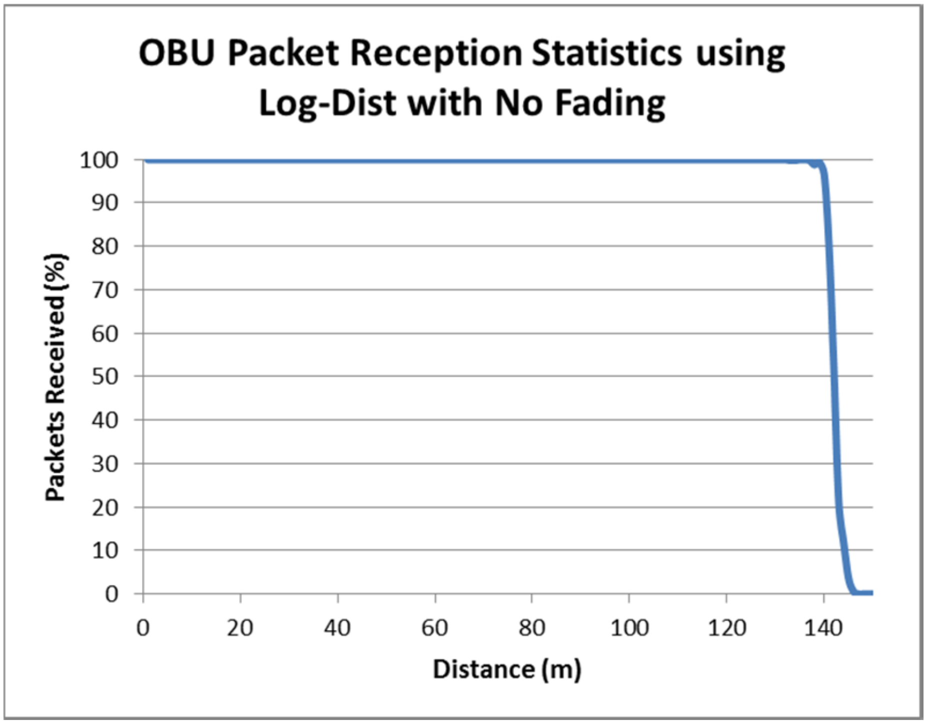


Figure 25. Packet reception plot using default values with log distance propagation loss

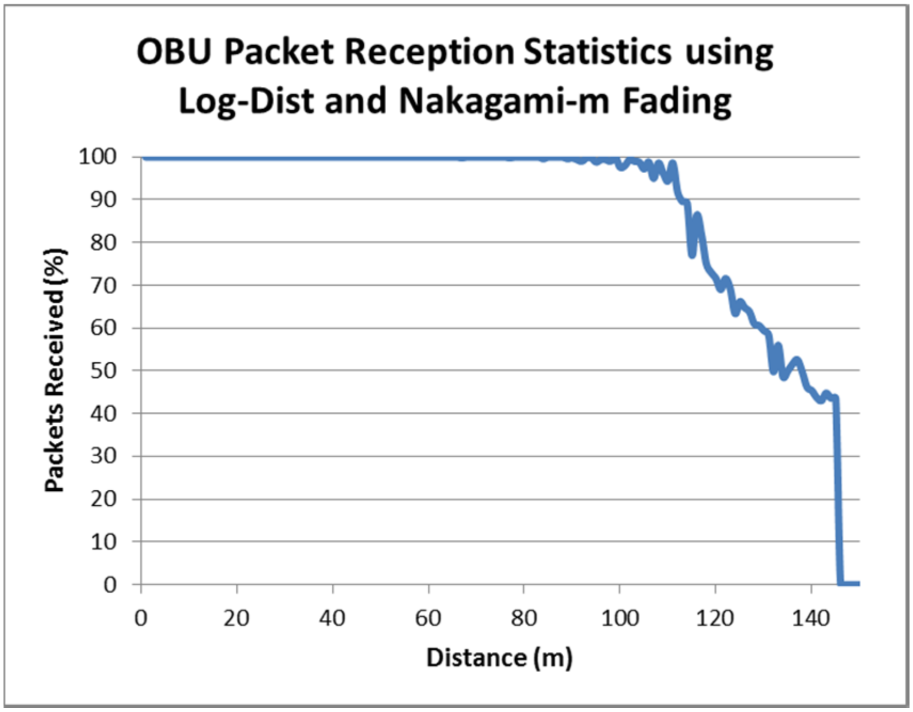


Figure 26. Packet reception plot with log distance propagation loss and Nakagami-m fading in an urban environment

4.6.4 Ns-3 Propagation and Fading Loss Conclusion

The use of simulators to provide insight into the workings of complex systems is an invaluable tool of the modern researcher. The ability to fine-tune a simulation configuration is a powerful asset to establishing causal relationships between design and performance. However the need to compare work across various efforts is an important necessity for true peer review. In this section, we have reviewed the nine propagation loss and the two fading models provided by ns-3.10 and evaluated their applicability to simulating vehicular networks. We proposed propagation loss and fading model parameter values to adapt ns-3 for VANET use. These proposed values were then validated through a series of ns-3 simulations within two percent of the mean values with a 95% confidence interval. It is our hope that these standardized values can provide a good reference for VANET researchers utilizing ns-3 (as well as potentially other simulators) as we all work towards a future of safer, more efficient, and more environmentally friendly vehicular travel.

For the remainder of this research, we adopted `ThreeLogDistance` propagation loss values of Table 14 and the Nakagami-m fading loss values of Table 15 consistent with whether we were simulating an urban or rural environment.

4.7 Mobility Models Overview

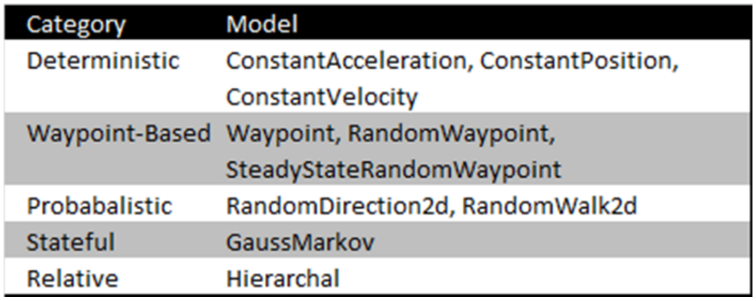
There are ten natively supported mobility models within ns-3.10 as summarized in Table 16. Each of the constant mobility models allows a node to travel from its starting position and travel with constant velocity or acceleration unless manually adjusted by code. For the `ConstantPositionMobilityModel`, the velocity is unable to be modified and is zero in all directions. For the `ConstantVelocityMobilityModel`, the velocity is set along the x, y, and z axes and does not change during the simulation unless manually done so. Similarly, the `ConstantAccelerationMobilityModel` involves providing each node with an initial velocity and then values for acceleration in all directions, which do not change unless explicitly later set to a new value.

In addition to these constant approaches, ns-3 also supports three way-point based models that use “trace” files of timed coordinates. The models in turn generate the appropriate velocity for each node from these files between each waypoint. The `WaypointMobilityModel` involves the nodes traversing the individually defined waypoints sequentially. The `RandomWaypointMobilityModel` works by viewing the waypoints as a pool and randomly picking a new destination among the waypoints available after a random pause once it reaches the current waypoint. The `SteadyStateRandomWaypointMobilityModel` develops this idea one step further for the special case when velocity, pause between advancing to the next waypoint, and the waypoints themselves are each uniformly distributed random variables.

Two random two dimensional mobility models are included with ns-3 and allow for more randomness in simulations while providing for controlled window of focus. The `RandomWalk2dMobilityModel` (also known as the Brownian Motion Model) allows the programmer to set each velocity (speed and direction) at random from user-provided random variables at either fixed distances or fixed amount of simulation time. In addition, if a node encounters one of the limits of the mobility window, the rebound of the node is in the opposite direction and speed. The `RandomDirection2dMobilityModel` is similar in allowing for each node to select from a random distribution of directions and speeds after a specified pause. However in this mobility model the nodes continue at that velocity until they encounter the edge of the mobility window at which time each one waits the same delay and then randomly selects a new velocity and repeats this behavior.

The final two mobility models represent particular cases for simulation. The `GaussMarkovMobilityModel` is a three dimensional model designed for aviation use and has both memory and randomness. In it, the programmer fixes a “TimeStep” and after each TimeStep the model uses the node’s current position and velocity (including pitch and yaw) to randomly select the next one based upon these values and the mean value, and a Gaussian random variable. The final native mobility model, the `HierarchalMobilityModel`, is for pack situations where “child” nodes follows a “parent” node, much like Pied Piper and the children of Hamelin. If the “parent” node moves north one meter, then all “children” nodes will move the same relative amount (one meter north) regardless of where they are located.

Table 16. Native mobility models of ns-3.10



Category	Model
Deterministic	ConstantAcceleration, ConstantPosition, ConstantVelocity
Waypoint-Based	Waypoint, RandomWaypoint, SteadyStateRandomWaypoint
Probabalistic	RandomDirection2d, RandomWalk2d
Stateful	GaussMarkov
Relative	Hierarchal

4.7.1 Mobility Models Analysis for Use in this Research

Given the ten mobility models of the preceding Section, we find that for fixed entities (i.e. RSUs), the `ConstantPositionMobilityModel` is the best choice. For highway scenarios of straight road, we used the `RandomDirection2dMobilityModel` as it allowed us to vary the speed for different traffic situations (no congestion, moderate congestion, and heavy congestion) but provide some randomness to the model. Since we were focused on particular geographic regions and wanted results for relatively fixed congestion across the entire simulation, the fact the vehicles reflected back into the road was beneficial and we considered this a one-for-one replacement (i.e. for every car that would have left the examined topography, another car entered). This preserved the traffic densities across the simulation. By using this same mobility model in an urban environment and only changing the direction to a limited number of choices all at right angles to the current direction of the OBU, we were able to replicate a downtown grid. Finally, for a more macroscopic and realistic simulation mobility model (but with no control of the congestion or roadway topography), we used the `WaypointMobilityModel` with ns-2 traces freely available from the Swiss Federal Institute of Technology – Zurcich [118] that were demonstrated in [119] and adapted for use in ns-3 by Dr. Michael Nowatkowski in [105].

4.8 Verification and Validation

Verification and validation is an important part of any simulation and involves ensuring that the simulation is realistic. By selecting appropriate propagation and fading loss as well as mobility models, we sought to incorporate realistic scenarios that would yield meaningful results. By using a widely available, free and open simulator that is presently relevant (it is currently under active development), all of our simulations can be replicated and the results we achieved validated. Furthermore, by using as much built-in functionality at the physical, media and access control, and network layers, we are able to rely on the stability of well researched and documented code versus our own, un-validated implementation. Finally, the code used in this research is an extensive extension of seed code previously used in the network and security architecture lab at Georgia Tech and has been vetted by other researchers and professionals in the VANET community, such as in [67].

4.9 Statistical Analysis [105]

Realistic simulation models are critical to achieving meaningful results. But in order to possess meaning, a good simulation must produce *statistically* meaningful results. Fortunately ns-3 has a built in pseudo-random number generator (PRNG) that allows for output that is correlated across various configurations of a particular simulation scenario and permits the use of simplified statistical analysis tools on the correlated output. This is accomplished by using a different substream within the random number generator (known as the "RngRun" value in ns-3). This was accomplished through scripts that ultimately varied this value using the SeedManager::SetRun(int RngRun) method.

Given this setup, statistical analysis was then accomplished to ensure the results were statistically significant using the methods described in [120-123] for correlated sampling. The same random number seed was used throughout all simulation runs, and the run number was incremented to use the next sub-stream of random numbers, as required by [124]. This synchronizes the random numbers to reduce variance between the scenarios tested and provided a more stable set of data across all scenarios. Of particular note is that the mobility models rely on these random number substreams when selecting their behavior and by using the same substreams, OBUs with the same mobility model installed would follow exactly the same paths. This is important because the paired-t comparison requires correlated sampling and independent replications.

Each experiment was run for multiple iterations to find several samples (Y) for the experimental criteria, as determined by the scenario itself and normally in the order of thirty runs. The next step was comparing each of the runs with each other. Since correlated sampling is used, the difference between results for each method is found and then averaged, resulting in the average difference between the methods, $\overline{D}$ (as in Equation 12), and the variance of the difference, S_D^2 (Equation 13). For these two equations, R is the total number of replications and *r* designates an individual simulation run.

$$\overline{D} = \frac{1}{R}\sum_{r=1}^{R}(Y_{r1} - Y_{r2}) \tag{12}$$

$$S_D^2 = \frac{1}{R-1}\sum_{r=1}^{R}(D_r - \overline{D})^2 \tag{13}$$

The null hypothesis, H_0, is that the two means of the different simulations are the same; thus the difference of the means would be zero, as shown in Equation 14. The alternative hypothesis, H_a, where the means are different, indicates that difference between the methods is statistically significant at the specified confidence interval, $(1 - \alpha)$, as shown in Equation 15. A confidence interval of 95% was used throughout this study.

$$H_0\text{: } \overline{D} = 0 \tag{14}$$

$$H_a\text{: } \overline{D} \neq 0 \tag{15}$$

The number of samples and the sample variance of the experiment runs under investigation are used to find the half-width of the difference between their means using Equation 16. The value of 0.05 is used for α, resulting in a 95% confidence interval for the half-width. The number of simulation runs for each experiment (R) is used to determine the degrees of freedom for the student-t distribution. [105]

$$half - width = t_{1-\frac{\alpha}{2},\ R-1} \cdot \sqrt{\frac{S_D^2}{R}} \tag{16}$$

The half width is then used with the difference of the sample means to determine if the experiments have a significant statistical difference. If $\bar{D} \pm half - width$ contains zero, then the null hypothesis cannot be rejected, indicating that there is not sufficient evidence that the experiments produced different means, i.e., that they are not different.

This mathematically rigorous methodology, which was similarly used by previous members of the network architecture and security lab of Georgia Tech, was applied to all of the simulation scenarios examined to ensure the data was statistically meaningful and conclusions drawn from the data had merit.

4.10 Simulation Computer Setup

As previously mentioned, the network simulator used was ns-3, which is software that involved the researcher coding various simulator applications and the simulation configuration in C++ and then compiling this code in conjunction with the ns-3 program on Linux-based operating system. The simulation experiments were designed on a Fedora-flavored Linux partition. Early and simpler experiments could be run with statistically significant results as defined in Section 4.9, on a series of computers overnight. As the experiments became more complex, additional computing power was required as it would take over a week using five computers to calculate a single data set. Fortunately, we had access to Georgia Tech's Partnership for an Advanced Computing Environment (PACE, [125]) high performance computing cluster which allowed 100's of cores to be harnessed simultaneously using portable batch system (PBS) scripts to interact with the PACE jobs scheduler. Massive simulation runs were then able to be conducted in as little as four hours depending upon PACE's available resources and system availability (it did experience some extended periods of down time during our research).

Data from the simulations consisted of a position log that could be used to follow the path of the OBUs and a second file which contained traces of all the packets sent and received by all nodes in the network. This latter file was then parsed using a MATLAB program and imported into Excel for further analysis.

CHAPTER 5

INVESTIGATED VANET IMPLICATIONS TO PN DISTRIBUTION

5.1 Introduction

As discussed throughout this dissertation, it remains the dual goal of vehicular networks to provide both security and privacy [68]. In fact, the goal of protecting a driver's location privacy is at the forefront of the minds of researchers, industry executives, and drivers given the proliferation of inexpensive technological tracking devices that can easily be used to monitor the movement of vehicles [126]. To protect against this threat within VANETs, pseudonyms remain the leading candidate as codified in the IEEE trial use standard 1609.2 [26]. Their distribution, however, is not a trivial issue given the vast number of mobile vehicles (or more precisely on-board units, OBUs) that comprise the network along with the fixed Road Side Units (RSUs). Of particular concern is their distribution in congested environments where contention for bandwidth will be great. In order to adequately address the PN distribution problem, one must examine when an OBU would be in a situation to need PNs.

5.2 Measuring an OBU's need for PNs

5.2.1 File Distribution

The concept of distributing files within a vehicular network remains an open research area that employs a wide range of potential solutions, from formal routing techniques to peer-to-peer file sharing. Much work has been done, such as Luo's urban routing protocol [127], the hybrid traffic routing and data collection scheme of [128], a peer-to-peer routing using Peer Computing based Ad Hoc On Demand Vector (PAV) as discussed in [129], and infrastructure-free file distribution with CoFFee [130]. An overall performance comparison of VANET routing protocols can be found in [131]. While we do not claim there is a "problem" with any of these approaches, we do share in the belief that the amount of bandwidth available within VANETs is quite limited [132].

5.2.2 Contribution

The contribution of this section is in introducing the intelligent reduction of channel load due to unnecessary PN refill thus leaving more bandwidth for other applications or for those OBUs with greater need. Here our goal is entirely different than simply data dissemination. Rather than adding to the research of *how* to route data, we examine the issue of *when* a vehicle should request data, specifically in the context of pseudonym refill. To the best of our knowledge, no other research has examined this question.

The work in this section demonstrates, through the use of ns-3 simulation, some methods that result in OBUs requesting PNs more intelligently, increasing the likelihood that vehicles with the greatest need will acquire pseudonyms. We do not simply examine existing PN distribution schemes, but rather introduce into the PN distribution process the novel question of "when should an OBU request PNs?" and demonstrate the impact of how these methods affect the answer to this question.

5.2.3 Background

The United Nations reported that by 2010, for the first time in their records, a majority of the world's population will live in an urban setting [133]. The Brookings

Institute declared that “rising traffic congestion is an inescapable condition in large and growing metropolitan areas across the world” [134]. Thus for vehicular networks to help reduce congestion, they must function in highly congested environments. This work looks at PN distribution along congested arterial roadways.

To determine what constitutes a reasonable measure of congestion, we analyzed traffic data from automatic traffic recorders (ATRs) as published by the State of Georgia (USA). From their study, we found that 29,419 vehicles passed through a given intersection in downtown Atlanta per 24 hour weekday [135]. We discounted night-time driving and sought to focus on the most congested portions of the day by reducing this to over only 12 hours, which yielded 2451.6 vehicles per hour or 20.43 over 30 seconds. We then modeled a single RSU slightly off-center in four square blocks of length 75 meters each, resulting in nine intersections (see Figure 27) containing an average of 184 vehicles. For this reason we ran simulations with 175, 200, and 225 vehicles. Of these, 100 were considered to be under observation for pseudonym refill and the remaining vehicles were engaged in background data transfer over the same shared channel.

Our work seeks to understand the relationship of PN distribution with the potential for other data, whether administrative or not, also being disseminated. We examined the successfulness of vehicles getting PNs as well as the effects of the PN refill process on the ability of other vehicles to receive non-PN data (labeled “background”) under the various techniques.

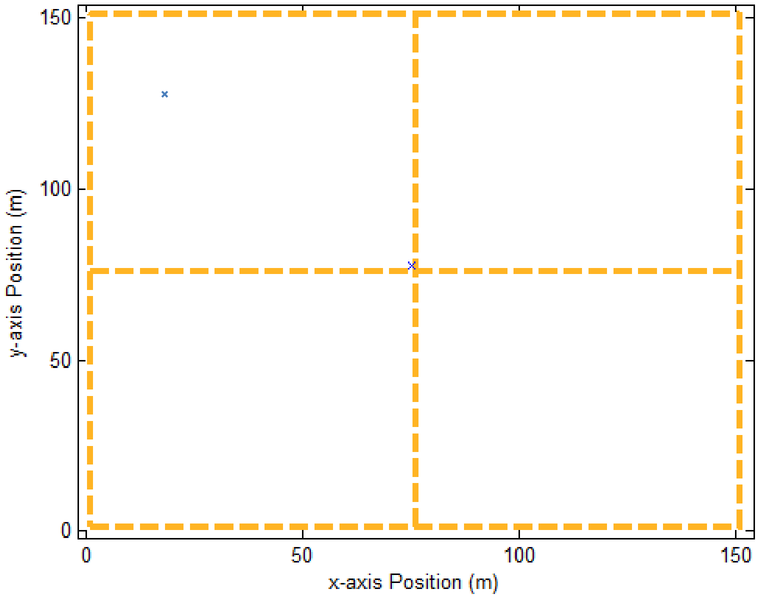


Figure 27. Simulation mobility topography.

5.2.4 Simulation Model Assumptions

For the purposes of this research, a series of assumptions were made in an effort to demonstrate the effect of various pseudonym distribution policies. When an OBU seeks PNs, it is going to need to request them from the certificate or registration authority [69, 90] and some time will have to elapse between this request and when the RSU can begin transmitting the PNs. We are assuming a best case scenario such that the PNs are already calculated and at the RSU for immediate distribution. In the next section, we examine techniques for disseminating PNs to the RSUs.

As for the vehicles themselves, in order to focus on congestion, each OBU's mobility is independent but constrained to make 90 degree turns (randomly selected) and stay within the 150 m x 150 m area of concern. It is assumed that for each vehicle that would have left this area, another one would take its place. Since we are ultimately concerned with the overall performance, aggregating the results provides the best indication of how various techniques would affect the overall system. We further assume that each OBU securely stores a cache of PNs on a trusted computing platform. We assume the use of each PN for one minute (validity period, as in [136]) and the possession of PNs for every hour of the day. Furthermore, we assume each OBU can store up to a year’s worth of PNs (60 minutes/hour x 24 hours/day x 365 days/year = 525,600 PNs/year). The amount each OBU starts with at the beginning of the simulation is evenly distributed and fixed across each run such that the vehicles have a wide range of PNs in their possession. The goal is for the vehicles with the fewest PNs to acquire the greatest number during the length of the simulation.

5.2.5 Simulation Communications Range

As discussed in Section 4.6, the exact range of VANET communications is difficult to determine. Physical and electrical factors such as terrain, vegetation, buildings, as well as policy and standards limit the effective range to maximize the number of supportable users. Consistent with our rationale in Section 4.6 and given that the work in this section focuses on urban congestion, we incorporated ns-3’s Three-Log propagation loss model with Nakagami-m fading to limit communication to 140 m [106].

5.2.6 Traffic Shape

In the simulations, we used a Poisson transmission rate of 100 packets per second of 1000 bytes each for the background traffic, which was sent to each OBU not involved in PN refill. PNs were distributed such that for each service channel interval in range when a request has been received, the RSU sends the requesting OBU 10 packets of 1000 bytes of data each (about 65 PNs total).

5.2.7 PN Distribution Techniques

In addition to possibly using wired PN transmission with regular periodic PN refill as in [39], some researchers have suggested that vehicles simply request PNs whenever they are in contact with an RSU [62, 65]. Concern lies with how many PNs a vehicle can obtain as well as the overall impact on bandwidth on neighboring vehicles. This issue is what the research outlined in this section seeks to gain insight upon. In so doing, three techniques are introduced and their performance impact measured through simulation with the decision by the OBU of when to request PNs being summarized in Table 17.

The first technique we implemented is a “baseline” (shown as BL in the figures) such that all vehicles constantly seek PNs (if they are one of the 100 PN-designated OBUs) or data from the RSU (if they are one of the remaining OBUs). Thus whenever a vehicle in this scenario encounters an RSU, it requests PNs and the RSU responds to that request. OBUs in this method request PNs even if they have a large supply of PNs stored. These requests both add to the channel contention and reduce the number of PNs other OBUs are able to receive since an RSU can only transmit a limited number of PNs per service channel interval.

The second technique we investigated used binary logic in determining whether an OBU should request PNs. An OBU requested additional PNs if and only if it stored less than a specified threshold of PNs onboard. We examined the threshold cases of 10, 20, 30, 40, 50, 60, 70, 80 and 90 percent "full." Thus if the threshold was set at 40% and an OBU only had 39% of its capacity of PNs, it would request PNs until it reached 40% full. On the other hand, using the same 40% threshold, a vehicle that was 70% full would not request PNs until its load went below the 40% threshold.

The final technique we investigated uses a probabilistic component to the refill question such that the likelihood an OBU sought additional PNs was inversely proportional to the number of PNs it possessed. In our method, the fewer PNs an OBU possessed, the more likely it would request PNs. The probabilistic component is further enhanced by utilizing a static threshold combined with a random number to control when a PN request is made. For example, if an OBU had 22% of its PN capacity and the static threshold was set at 25%, the OBU would uniformly select a random integer between zero and 25 and if that number was greater than its present capacity the OBU would request PNs during that service channel interval. On the other hand, if the threshold was 25% and it had 40% of its PN capacity, the random number chosen would never exceed 25 and it would never request PNs (until its cache was reduced to below 25%). We examined threshold cases of 25, 50, 75, and 100 percent.

Table 17. PN request pseudocode.

Method	OBU Request PN Pseudocode
1	`Always request PNs`

2	`IF % full < threshold`
	`THEN request PNs`

3	`RND = RandomNumber[0, Threshold]`
	`IF (% full < threshold) AND (RND > % full)`
	`THEN request PNs`

5.2.8 Model Metrics

In order to shed some light on the issue of PN distribution in congested environments and the performance of the various proposed techniques, four metrics are introduced. (1) The first is the total throughput of network background data as well as that value scaled per OBU. This looks at how much data the other vehicles are able to acquire in the presence of 100 vehicles focused solely on PN refill. Given that those vehicles that require PNs receive them, an increase in this number demonstrates improvement. (2) The second metric is the number of PNs received by the PN refill OBUs. Given that all of these vehicles are examining their PN store and potentially seeking PNs, higher numbers are better. (3) Another metric is the maximum number of PNs any OBU received. Given that a portion of the vehicles are very low on PNs, the more this number increases the more improvement we witness. (4) Finally, we group the PN refill OBUs in bins based upon their fill status (number of PNs divided by the maximum number of PNs that can be stored) and look at the performance of the various techniques on each of these bins. The greater this number for low percentage bins, the more effective a particular technique is in providing PNs to vehicles closer to running out.

5.2.9 Simulation Results

This section outlines the results achieved through ns-3 simulation. All values were derived following the methods outlined in [99] to obtain a 95% confidence interval with a half-width of the mean simulated value of 5% for the baseline and static threshold scenarios and 10% for the probabilistic with static threshold scenario. Each simulation run lasted 30 seconds of simulation time. In each scenario, one hundred vehicles were involved in the PN refill process. These vehicles either requested PNs the entire duration of the simulation, if they had less than a certain threshold, or only randomly if they had less than a certain threshold. The baseline method is on the far left, the static threshold method is in the middle, and the probabilistic with static threshold is on the right for this and all graphs.

Background Data Traffic

Figure 28 presents the average results across all methods and for all three OBU traffic densities of 175, 200, and 225 vehicles. For the baseline case, as additional vehicles were added, the total amount of background data received increased, but the amount each OBU received decreased, most likely due to increased channel contention. The total background traffic in the static threshold method increased as additional vehicles were added when the static threshold was greater than approximately 50%. For static threshold values below approximately 30%, the amount of bandwidth available for background traffic decreased as the vehicle density increased. The probabilistic with static threshold method showed a similar trend. Figure 29 demonstrates that in all cases the amount of background data decreased, on average, per vehicle involved.

Pseudonym Refill

Figure 30 presents the total pseudonym data traffic throughput for each of the methods and each of the vehicle traffic densities. In every case, as the vehicle density increased, the average number of PNs that were able to be acquired decreased. Surprisingly, the baseline data represented the

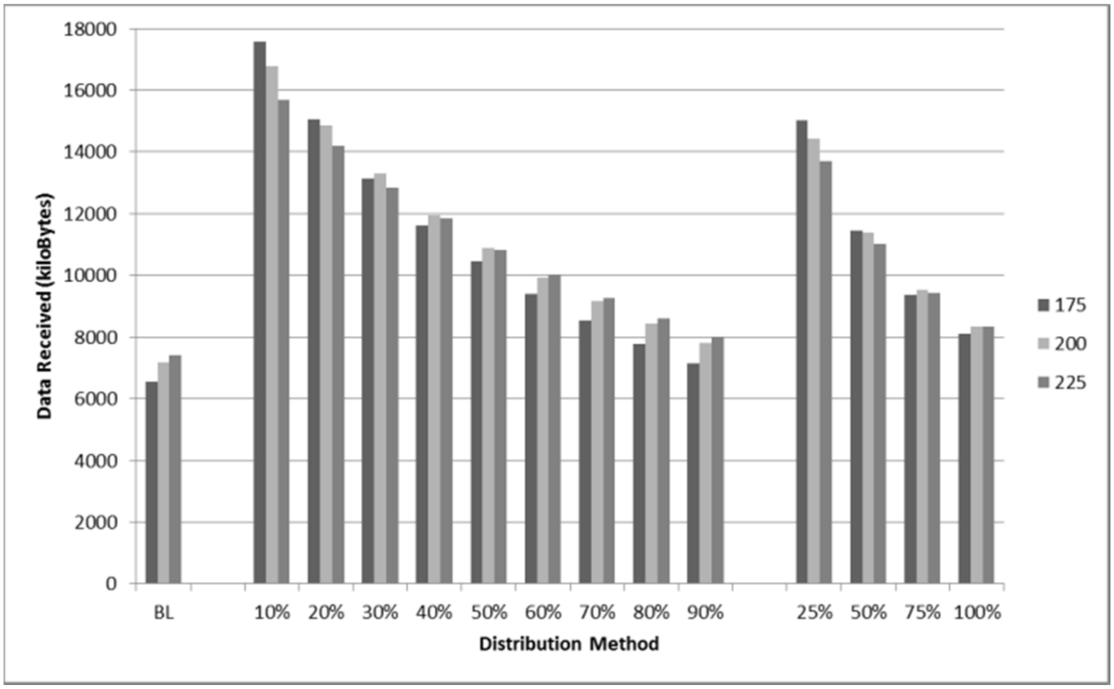


Figure 28. Total background data received.

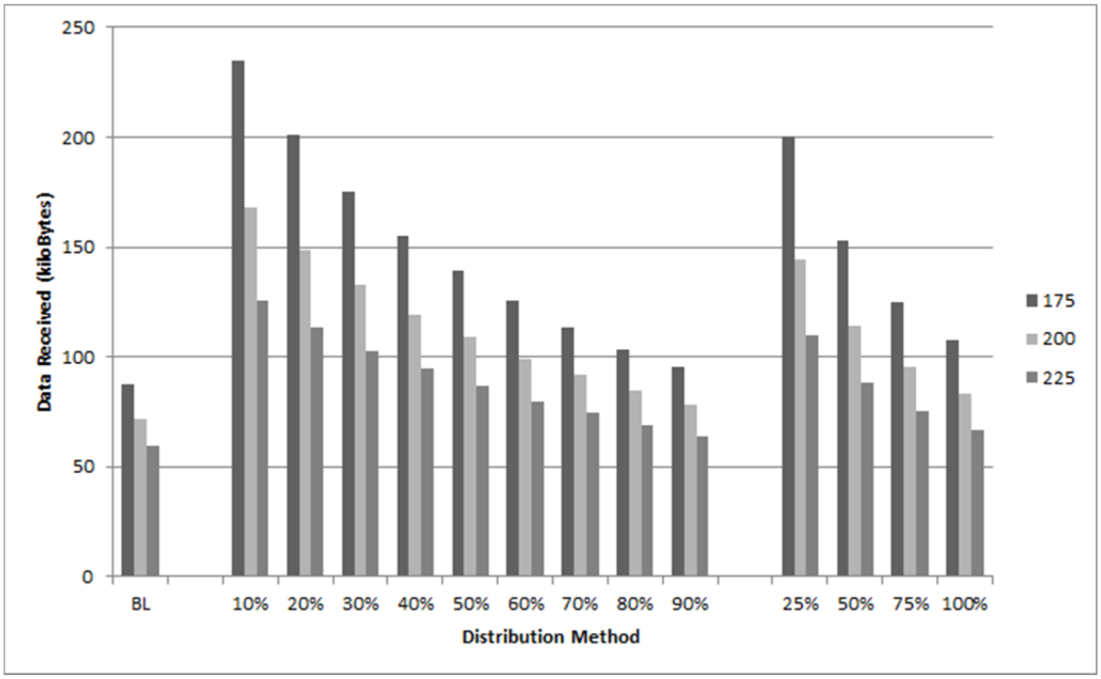


Figure 29. Background data received per background OBU.

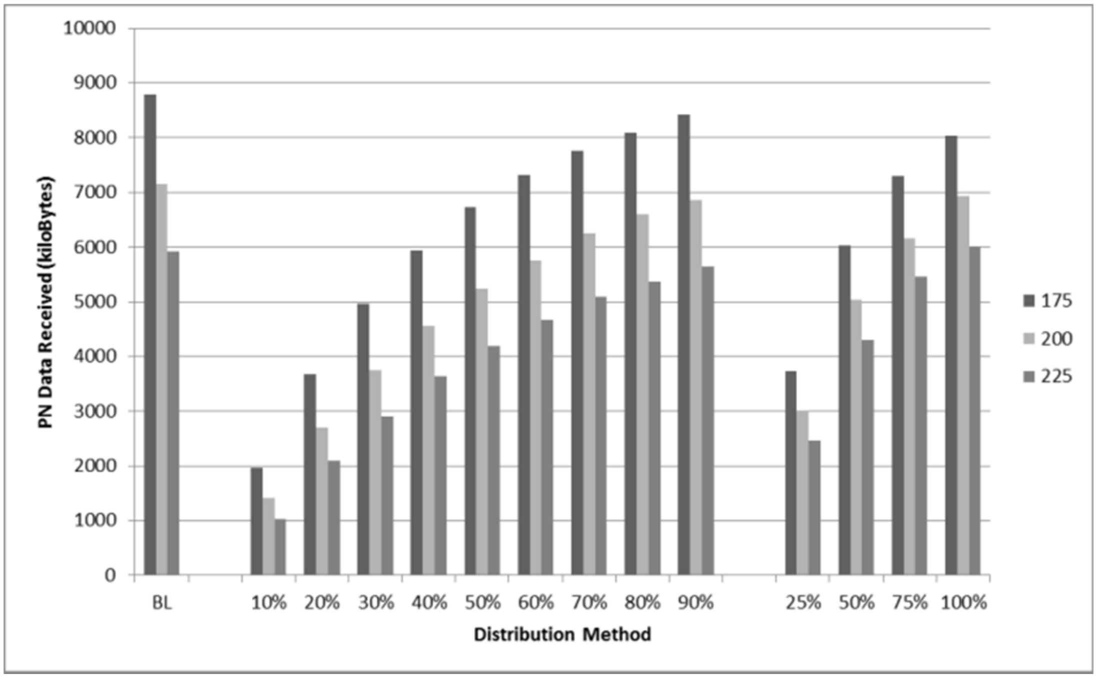


Figure 30. Total PN data received.

scenario whereby the maximum number of PNs were able to be distributed compared with the other methods. One might conclude that it represents the “best” approach to PN distribution, but as will shortly be seen, this is directly dependent on one’s definition of “best” and probably does not represent the best approach.

A final look at the total received data (Figure 31) reiterates that as expected an increasing number of OBUs results in a decreased overall throughput. What is less obvious from the previous graphs is that even with increased vehicle density, it is possible to achieve increased performance (i.e. greater overall data throughput) by limiting which vehicles seek PNs. For example, in the second distribution method shown in Figure 31 in the extreme case of only vehicles with less than 10% of PNs requesting refill, more data is received overall with 225 OBUs than in the 90% case with only 175 OBUs.

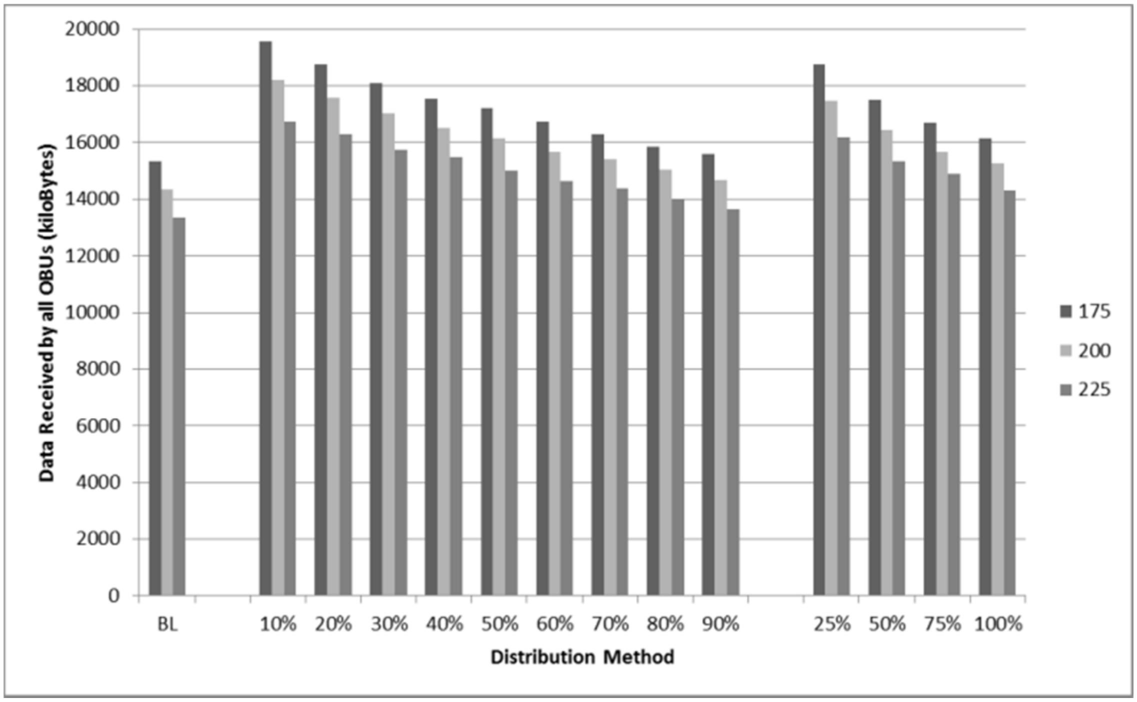


Figure 31. Aggregate background and PN data.

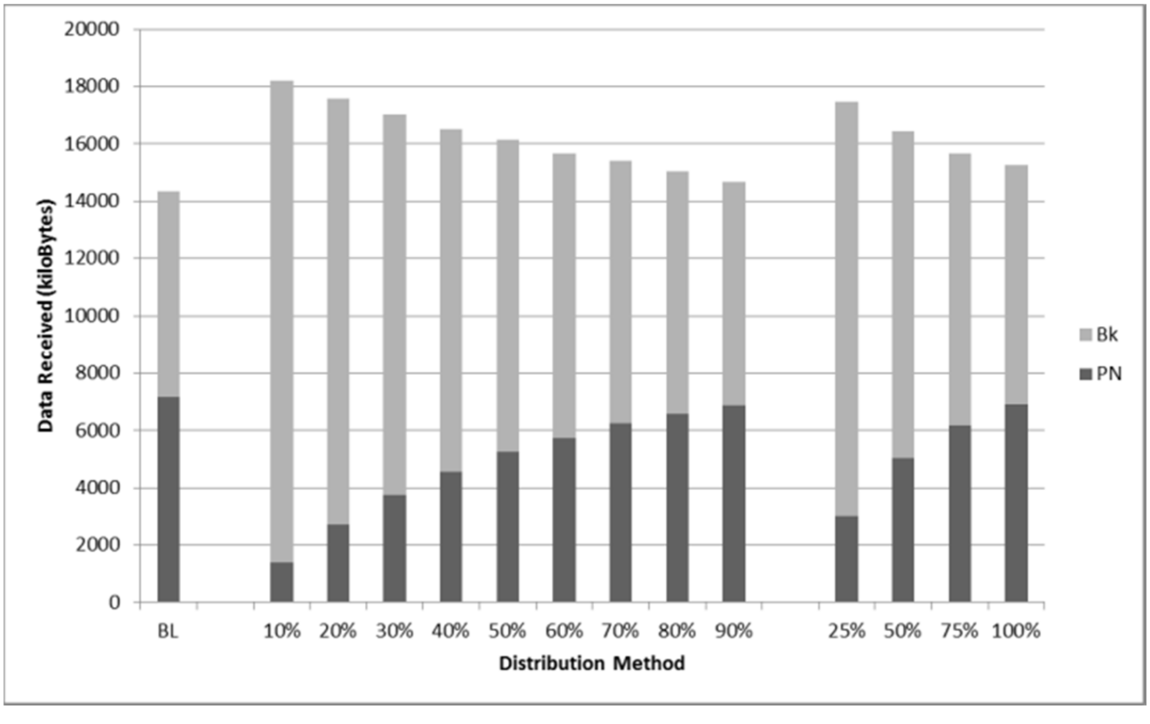


Figure 32. Total data received broken down by data type (200 OBU case).

In order to show the impact of the various PN distribution techniques on other background applications (whether administrative or otherwise) sharing the same channel, Figure 32 shows the relative data throughput for the 200 OBU case.

Maximum number of PNs Distributed

While overall throughout is important, for the purposes of PN distribution, it may be necessary to maximize how many PNs one can distribute to a single vehicle. Figure 33 demonstrates this result. As can be seen, by reducing the number of vehicles requesting PNs, even in the presence of other data traffic, the number of PNs received by the remaining PN OBUs increases.

Distribution of PNs Distributed

As an extension of viewing the maximum number of PNs distributed, it is also instructive to examine how the distribution of PNs affects vehicles with various levels of stored PNs. Figure 34 illustrates this point and shows that when all vehicles are equitably seeking PNs, as in the baseline case, they each receive a relatively equal amount. However, a relatively equal distribution of PNs may not be the goal when vehicles with very few PNs are present. In such circumstances, a method that discriminates the PNs based upon their need is better suited to deliver more PNs to these vehicles (and may result in the greatest number of PNs being delivered overall – but not the most overall data). Figure 35 adds emphasis to this somewhat surprising result by illustrating a side-by-side comparison of PNs delivered to sets of OBUs whose members started with less than 50% of their PN capacity.

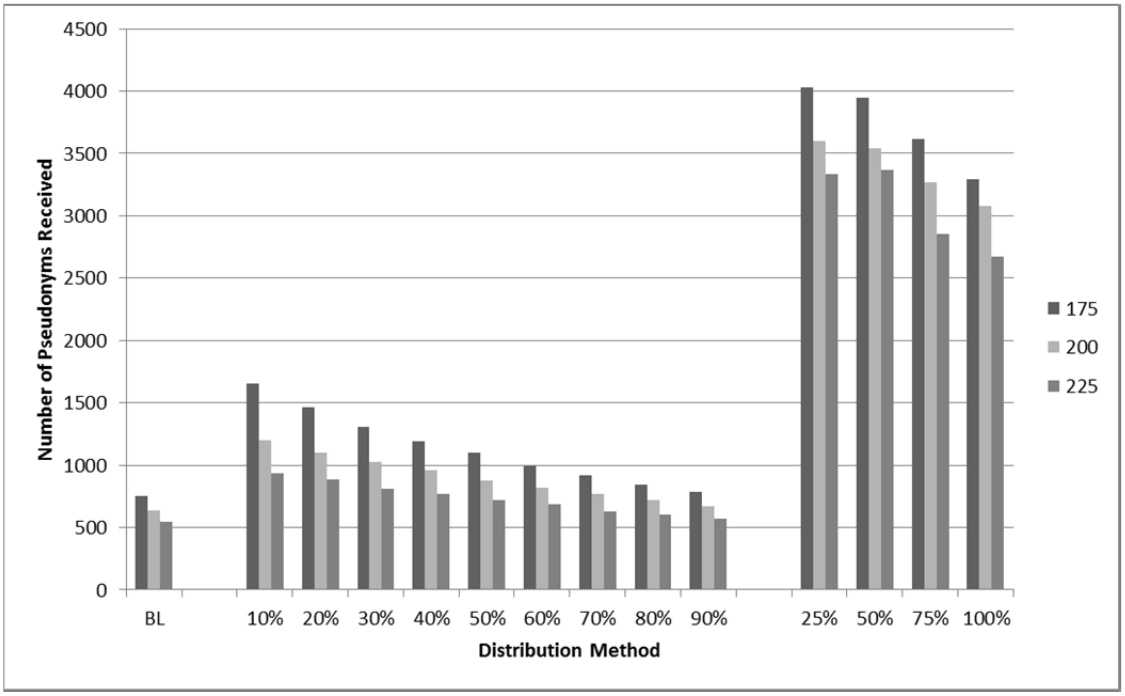


Figure 33. Maximum number of PNs received by a single OBU.

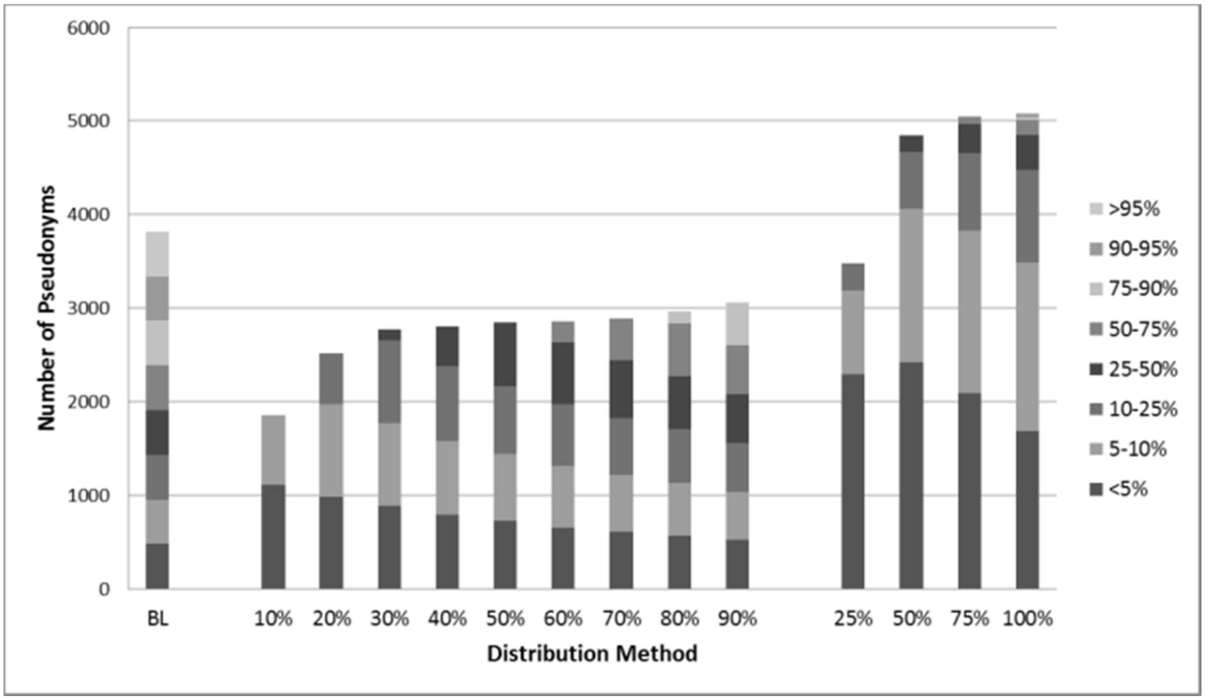


Figure 34. Breakdown of PNs received by OBU PN fill level (200 OBU case).

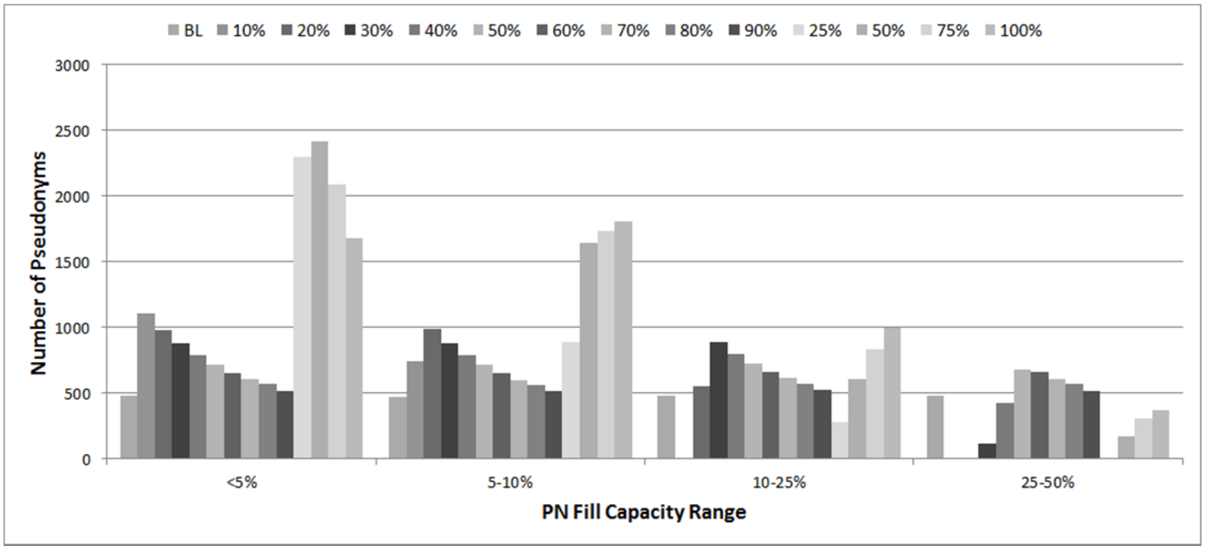


Figure 35. Closer examination of those OBUs starting with the fewest PNs.

Summary of Results

From the foregoing discussion, it has been demonstrated in densely populated vehicular environments that the number of PNs distributed increases by reducing the number of OBUs accessing the shared medium. The best way to reduce who is seeking PNs ought to be based upon need, and of the three methods introduced, the last method performed the best. The final method with a threshold of 50%, for example, allowed for more total data throughput than the baseline case or the static 50% threshold, as shown in Figure 32. More importantly, method 3 provided the greatest number of PNs to those OBUs closest to being empty, as shown in Figure 34; thus it could be argued that it provides the best balance of overall data and proper PN distribution.

5.2.10 Section Summary

As has been shown in this section, an equitable distribution policy may not be "best" in providing PNs to vehicles. Such a policy may make it more likely that those cars with the fewest PNs do not receive a sufficient number of PNs to last before reaching another RSU. In 30 seconds with an RSU in the urban environment we simulated, the baseline method of granting equal priority to PN distribution resources only provided a maximum of 650 PNs (less than half a day's worth) over 30 seconds in the 200 OBU case.

In the presence of congestion, only a limited number of PNs can be distributed. When only the OBUs that "urgently" need PNs request them, those "urgently" needing PNs receive more than compared to the equitable distribution policy scenario. Thus the best performance in terms of PN distribution among the three techniques we examined was achieved with a 25% to 50% static threshold (which eliminated 75% to 50% of the OBUs vying for PNs) coupled with a request of PNs which was directly proportional to need as measured by the PN storage level of each OBU. Such a method resulted in almost eight times the number of PNs being distributed exclusively to those with less than half of their PN capacities filled.

5.3 Effect of Data Transmission Prioritization

A method within networking to optimize the use of bandwidth and provide, in some cases, service guarantees is known as Quality of Service (QoS). While normally thought of as a means to ensure real time applications, such as voice and video, have priority on a network so latency is minimized, the use of QoS can more broadly be used to provide certain data transmissions a greater likelihood of successful reception. For wireless networks, enhanced channel data access (ECDA) is codified in IEEE standard 802.11e [137] for general wireless networks and amended for use in vehicles by 802.11p [138]. While others have investigated the use of QoS for routing, such as [139-141], we are unaware of any studies of using QoS in the distribution of PNs from the VANET infrastructure to OBUs in the vehicular network.

5.3.1 Contribution

This work extends the research conducted in the previous section into various methods to distribute PNs within a downtown environment consisting of roads forming a grid. This work specifically looks at two additional QoS-related methods and their impact in the same inner city environment. Furthermore, both the previous non-QoS and current QoS-related methods are examined in a new environment: an urban controlled-access motorway. In support of this effort to enumerate methods to improve pseudonym distribution in congested environments, this work demonstrates through the use of ns-3 [95] simulation, an additional, novel technique that can be viewed as a "light-weight" QoS method. The goal of this method of reduced complexity and requiring no lower layer support is to allow for greater utilization of VANET channels while increasing the likelihood that those vehicles with the greatest need will acquire the pseudonyms they require. This section demonstrates that such a method can achieve almost identical performance to the full QoS implementation.

5.3.2 Background

Traffic Congestion - Highway

To determine what constitutes a reasonable measure of congestion for this portion of our research for a highway scenario, we analyzed traffic data from automatic traffic recorder (ATR) 5468 as published by the State of Georgia (USA) Department of Transportation. From this study, we found that 277,155 vehicles traveled past a point per 24 hour weekday on a roadway classified by the State of Georgia as an “urban interstate principal artery” that lies in downtown Atlanta and is shown in Figure 36 [135, 142]. In order to focus on a highly congested scenario, we used this entire count of vehicles but restricted it over a mere six hours. This yielded 46,192 vehicles per hour or approximately 385 vehicles over 30 seconds. We then modeled a single RSU slightly off-center of 14 traffic lanes (reflecting this portion of the highway) stretching 280 meters, 140 meters in each direction from the RSU. Thus for our topography, the average number of vehicles we would expect to see over a simulated interval of 30 seconds is 385 and for this reason we ran simulations with 400 vehicles. Of these, all were considered to be under observation for pseudonym refill.

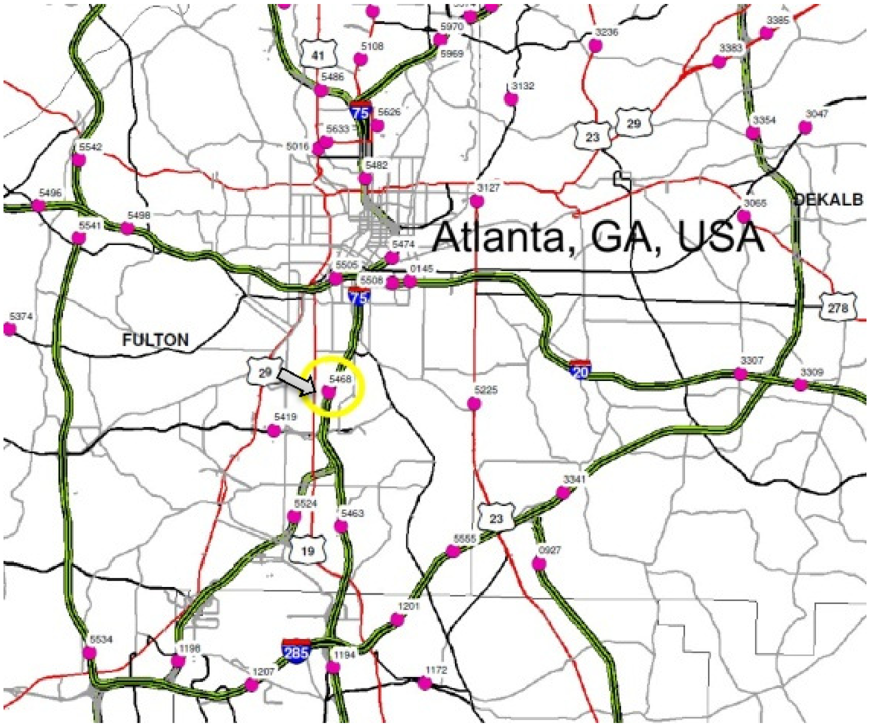


Figure 36. Location of ATR 5468 along interstate 75/85 in Atlanta, GA.

Traffic Congestion – Inner City

A similar analysis was conducted for the inner city case without quality of service functionality in our work in [143]. While that work did not include QoS or a highway topography, it did provide a baseline of PN distribution from which the presently discussed work will be compared to in order to understand the effects of QoS in a congested, grid-like roadway topography. In addition, and in contrast to the highway scenario, the inner-city scenario looked at vehicle densities of 175, 200, and 225 vehicles. In recognition of the potential for shared applications within a single service channel, PN refill activity was limited to only the first 100 vehicles. The remaining vehicles were engaged in background data transfer over the same shared channel.

Our work seeks to understand the relationship of PN distribution with the potential for other data, whether administrative or not, also being disseminated, as well as looking at the exclusive use of a channel for PN distribution. Thus for both topographies we examined the successfulness of vehicles getting PNs and for the inner city, the effects of the PN refill process on the ability of other vehicles to receive non-PN data (labeled "background") under the various techniques.

5.3.3 Simulation Model Assumptions

A series of assumptions were made in an effort to demonstrate the effect of various pseudonym distribution policies. When an OBU seeks PNs, it is going to need to request them from the certificate or registration authority [69, 90] and some time will have to elapse between this request and when the RSU can begin transmitting the PNs. We are assuming a best case scenario such that the PNs are already calculated and at the RSU for immediate distribution.

As for the vehicles themselves, in the highway topography, the vehicles travel in a straight line at a speed randomly selected between 5 and 20 MPH (2.235 and 8.941 m/s). Speed changes occur every seven seconds to represent a typical highly congested scenario. In the inner city grid topography, each OBU's mobility is independent but constrained to make 90 degree turns (randomly selected) and stay within the 150 m x 150 m area of observation. It is assumed that for each vehicle that would have left this area, another one would take its place. Since we are ultimately concerned with the overall performance, aggregating the results provides the best indication of how various techniques would affect the overall system.

We assume that each OBU securely stores a cache of PNs on a trusted computing platform. We assume the use of each PN for a one minute validity period, as in [136], and the possession of PNs for every hour of the day. Furthermore, we assume each OBU can store up to a year's worth of PNs (60 minutes/hour x 24 hours/day x 365 days/year = 525,600 PNs/year). The amount of PNs each OBU starts with at the beginning of the simulation is evenly distributed from zero to the 525,600 and fixed across each run such that the vehicles have a wide range of PNs in their possession. We used the same communication range values as in Section 5.2.

In the inner city simulations, we used a Poisson transmission rate of 100 packets per second of 1024 bytes each for the background traffic, which was sent by the RSU to each OBU not involved in PN refill. PNs were distributed such that for each service channel interval in range when a request has been received, the RSU sends the requesting OBU 10 packets of 1000 bytes of data each. IEEE 1609.2 defines each PN to be 153 bytes and we assume that PNs can span multiple transmissions and can be concatenated together [26].

5.3.4 PN Distribution Techniques

In addition to possibly using wired PN transmission with regular periodic PN refill as in [39], some researchers have suggested that vehicles simply request PNs whenever they are in contact with an RSU [62, 65]. Concern lies with how many PNs a vehicle can obtain as well as the overall impact on bandwidth on neighboring vehicles. This issue is what the research outlined in this section seeks to gain insight upon, specifically with the use of QoS or a QoS-like mechanism. In so doing, five techniques are introduced and their performance impact measured through simulation. Given that VANETs have yet to be deployed, none of these techniques have currently been proposed for use.

The first technique we implemented is a “baseline” (shown as BL in the figures) such that all vehicles constantly seek PNs (if they are one of the PN-designated OBUs) or data from the RSU (if they are one of the background traffic OBUs). The second technique we investigated was a binary logic or static threshold method such that vehicles only sought additional PNs if they had less than a specified threshold of PNs stored onboard. This was performed for the threshold cases of 10, 20, 30, 40, 50, 60, 70, 80 and 90 percent “full.” Thus if the threshold was set at 40% and an OBU only had 39% of its capacity of PNs, it would request PNs until it reached 40% full.

The third technique we investigated applied a probabilistic component to the refill question such that the likelihood an OBU sought additional PNs was inversely proportional to the number of PNs it possessed. For this reason we refer to it as the probabilistic with static threshold method. The fewer PNs an OBU possesses, the more likely the OBU will request PNs. The probabilistic component utilizes a static threshold combined with a random number to control when a PN request is made. As an example, if an OBU had 22% of its PN capacity and the static threshold was set at 25%, the OBU would uniformly select a random number between zero and .25 and if that number was greater than its present capacity the OBU would request PNs during that service channel interval. On the other hand, if the threshold remained 25% and it had 40% of its PN capacity, the random number chosen would never exceed .25 and it would never request

PNs until its cache was reduced to below 25%. We examined threshold cases of 25, 50, 75, and 100 percent.

The fourth method of PN distribution implemented a QoS-like mechanism to underlying hardware with no QoS support (in ns-3, this was implemented through the use of the `NqosWifiMacHelper` class). This "light-weight" approach simply assigned a "roughly equivalent access category" (reAC) to each transmission based upon the fill level of an OBU's PNs. The goal here is not to replace the full functionality of QoS, but rather implement a simple and straightforward means of giving priority to certain packets while preserving some sense of the values used in QoS. These reAC's then provide a range of delay times before an OBU or RSU would transmit information comprised of a fixed value (equivalent to arbitrary inter-frame space number, or AIFSN) and a randomly selected value for the "roughly equivalent contention window" (reCW). The values used in this approach are enumerated in Table 18. The sum of the reAIFSN and randomly chosen reCW are then multiplied by the slot time (defined as 16 μs in IEEE 802.11p standard for MAC QoS enhancements for wireless access in vehicular environments [138]). This fourth method was conducted such that the thresholds for each roughly equivalent access category was varied and are given in Table 19. Note that the last row represents thresholds for one day, one week, and one month. Thus in the first case, an OBU that is 20% full would use reAC VO while one 85% full would use reAC BK. In the fourth case, an OBU that has 2% of the possible number of PNs that can be stored would us reAC VI but should that OBU achieve a level of 2.5%, it would switch to using reAC BE until it had reached a level of 5%.

Table 18. Values for roughly equivalent method of quality of service.

reAC	Description	reCWmin	reCWmax	reAIFSN
BK	Background	0	15	7
BE	Best Effort	0	7	3
VI	Video	0	3	2
VO	Voice	0	1	2

Table 19. Thresholds for each reQoS and QoS trial.

Case	VO Threshold	VI Threshold	BE Threshold
1	25%	50%	75%
2	10%	25%	50%
3	5%	10%	20%
4	1%	2.5%	5%
5	0.3%	1.9%	8.3%

The final method analyzed is the implementation of IEEE 802.11e as amended by 802.11p as provided by ns-3. In order to implement this in the real world, all participants in the VANET will have to support QoS. This also adds some overhead to the network and could potentially open the network to abuse by nodes using higher priorities than appropriate. For this reason, it is unknown whether VANETs will support total QoS functionality. The same five cases listed in Table 19 were used for this QoS method.

5.3.5 Model Metrics

In order to shed some light on the issue of PN distribution in congested environments and the performance of the various proposed techniques, four metrics were used. (1) Total throughput of network background data is the first and it applies only to the inner city grid topography. This looks at how much data the other (75, 100, or 125) vehicles are able to acquire in the presence of the 100 vehicles focused solely on PN refill, as discussed in 0. To compare among the different vehicle densities, this metric has been normalized to the number of vehicles involved. Given that those vehicles that require PNs receive them, an increase in this number demonstrates improvement. (2) The second metric is the number of PNs received by the PN refill OBUs. Given that all of these vehicles are examining their PN store and potentially seeking PNs, higher numbers are better. (3) Another metric is the maximum number of PNs any OBU received. Given that a portion of the vehicles are very low on PNs, the more this number increases the more improvement we witness. (4) Finally, the last metric quantifies the increase of PNs over the simulation based on how many PNs an OBU has at the start of the simulation. We group the PN refill OBUs in bins based upon their percent filled status at the start of the simulation run (number of PNs divided by the maximum number of PNs that can be stored) and look at the performance of the various techniques on each of these bins. The greater this number for low percentage bins, the more effective a particular technique is in providing PNs to vehicles closer to running out of them.

5.3.6 Simulation Results

This section outlines the results achieved through ns-3 simulation of the five methods discussed in section 5.3.4. All values were derived following the methods outlined in [99] to obtain a 95% confidence interval (CI). The upper and lower CI bounds for each measurement are displayed on the graphs directly. Each simulation run covered 30 seconds of simulated time.

Highway Scenario: Pseudonym Refill

In each of the methods for the highway scenario, four hundred vehicles were involved in the PN refill process. These vehicles either requested PNs the entire duration of the simulation (although potentially with different delays/access categories) or only if they had less than a certain threshold of PNs stored (sometimes with a certain randomness included). Figure 37 presents the total pseudonym data traffic throughput for each of the methods. In terms of the first two methods after the baseline, the increase of the threshold resulted in fewer PNs being distributed. In terms of the roughly equivalent QoS and true QoS methods, tightening the threshold for higher access categories resulted in more PNs being distributed above a certain threshold. With the thresholds too stringent, fewer PNs were actually distributed. Overall, all four techniques at any setting distributed more PNs than the baseline method and the greatest number of PNs were distributed using the 10% static threshold followed by the 5%-10%-20% QoS and QoS-like methods which had nearly identical performance, and then the 20% static and 25% dynamic threshold methods which also had very close performance.

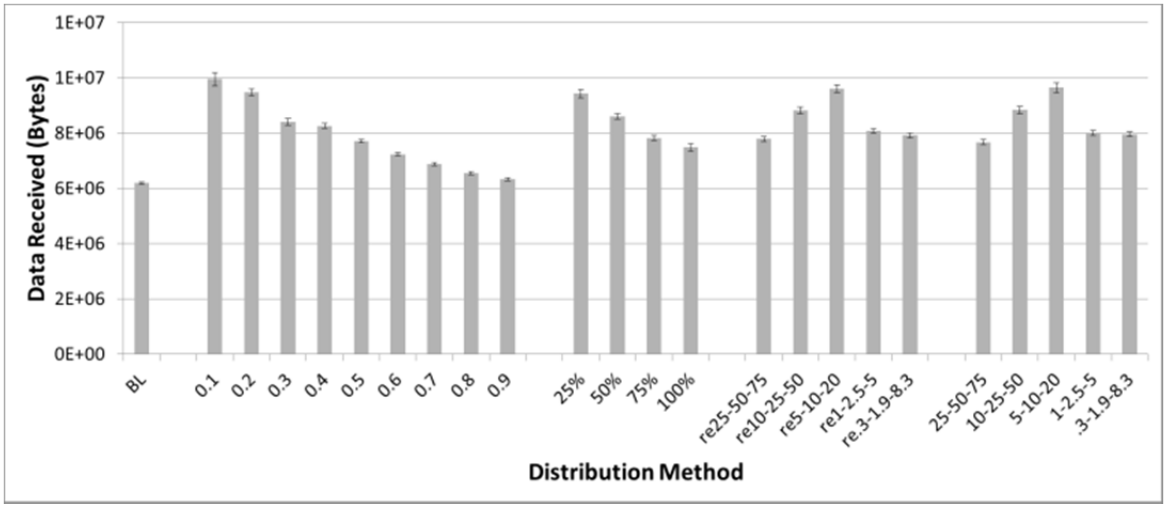


Figure 37. Total PN data received.

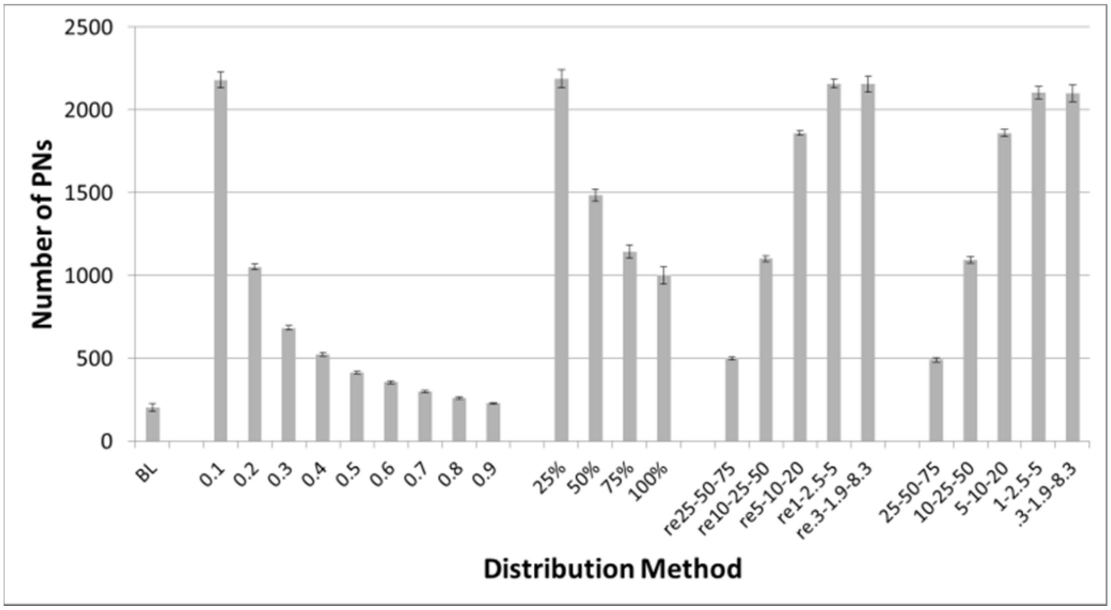


Figure 38. Maximum number of PNs received by any single OBU.

Highway Scenario: Maximum number of PNs Distributed

As discussed in the previous section, for the purposes of PN distribution, it may be necessary to maximize how many PNs one can distribute to a single vehicle. Figure 38 demonstrates this result. The maximum number of PNs were delivered to a single vehicle using the 25% dynamic threshold method. The 10% static threshold was second best in this metric. The 1-2.5-5 and .3-1.9-8.3 QoS-like methods were third best with the same thresholds being approximately equal in the true QoS method coming in fourth.

Highway Scenario: Distribution of PNs Distributed

As an extension of viewing the maximum number of PNs distributed, it is also instructive to examine how the distribution of PNs affects vehicles with various levels of stored PNs. Figure 39 illustrates this point and shows that when all vehicles are equitably seeking PNs, as in the baseline case, they each receive a relatively equal amount.

However, a relatively equal distribution of PNs may not be the goal when vehicles with very few PNs are present. In such circumstances, a method that distributes the PNs based upon their need is better suited to deliver more PNs to these vehicles (and may result in the greatest number of PNs being delivered overall – but not the most overall data). Figure 39 also demonstrates that a strategy to how QoS might be implemented is an important factor. Setting the thresholds too liberally such that too many vehicles are transmitting at high priority results in fewer PNs being distributed. Setting the threshold too tightly can also have a deleterious effect. Interestingly, these results mirror those of the previous metric.

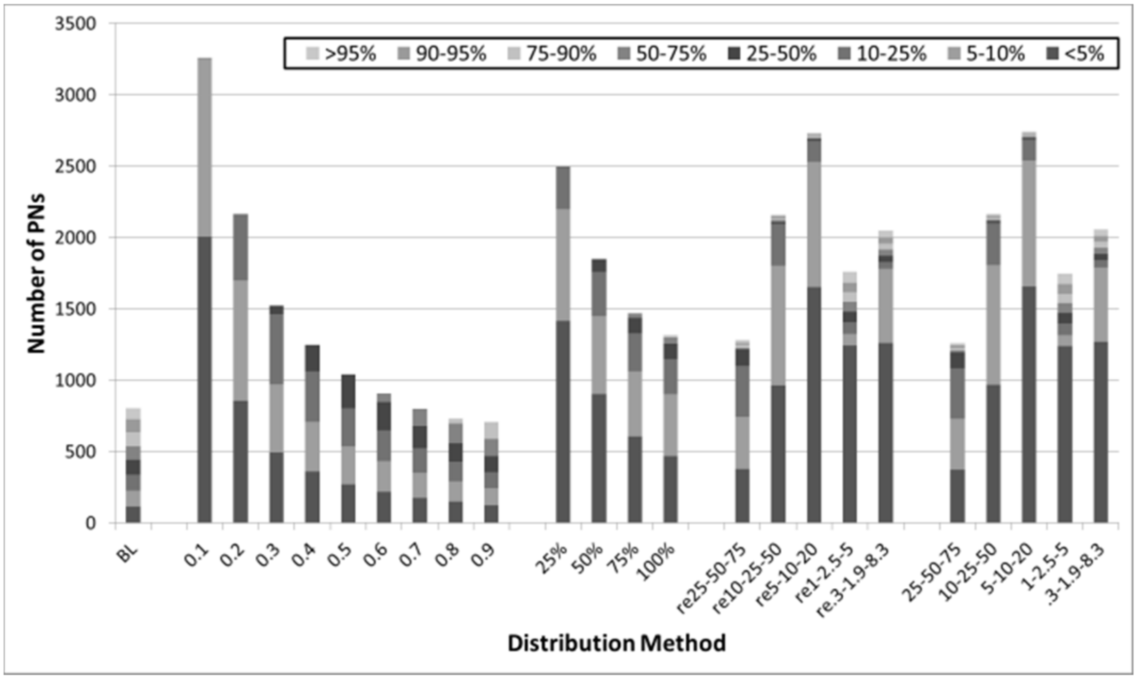


Figure 39. Breakdown of PNs received by OBU PN fill level (200 OBU case).

Inner City Scenario: Background Data Traffic

Figure 40 presents the average results of total received background data across all five methods and for all three OBU traffic densities of 175, 200, and 225 vehicles for the inner city topography. We see that the per OBU data decreases without exception for the baseline, static, and probabilistic methods as the number of vehicles seeking background data increases. In the QoS-like and QoS cases, there is a slight increase in the amount of background date received for 125 background OBUs compared to only 100, but both receive less than the 75 background OBU case. The most background data is transmitted in the 10% static threshold case followed by the 20% static and 25% static with probabilistic threshold cases.

Inner City Scenario: Pseudonym Refill

In each inner city scenario, one hundred vehicles were involved in the PN refill process. With limited bandwidth, a portion of what is available is bound to be used for PN data transmission and a portion for the background data. Figure 41 illustrates, for the 200 OBU case, how these proportions change for the various methods. In the QoS-like case and especially in the QoS case, the background data receives the least proportion of the available bandwidth.

Figure 42 presents the total pseudonym data traffic throughput for each of the methods and each of the vehicle traffic densities. In every case except the first three QoS thresholds, as the vehicle density increased, the average number of PNs that were able to be acquired decreased. In terms of the first three methods, the baseline data represented the scenario whereby the maximum number of PNs were able to be distributed. However when the pseudo-QoS and true QoS methods are compared to these, the QoS-associated methods demonstrate a marked increase in the amount of PN data delivered.

Inner City Scenario: Maximum number of PNs Distributed

Figure 43 demonstrates for the first three methods that reducing the number of vehicles requesting PNs, even in the presence of other data traffic, the number of PNs received by the remaining PN OBUs increases. For the final two methods where all vehicles are requesting PNs but with different priorities, we again see a similar but not absolute trend.

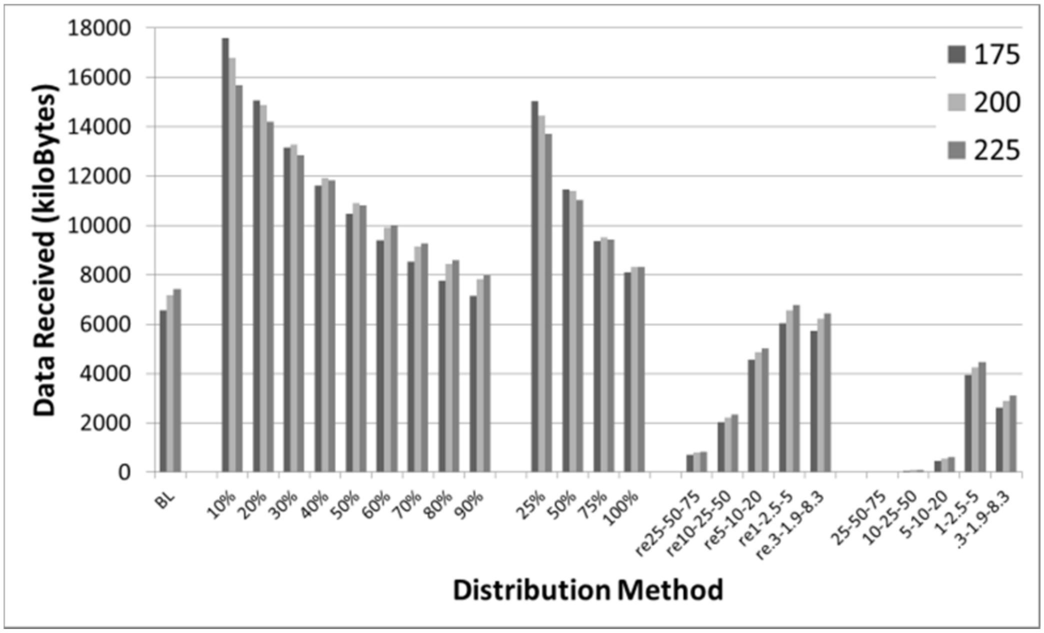


Figure 40. Total background data received (Normalized per OBU).

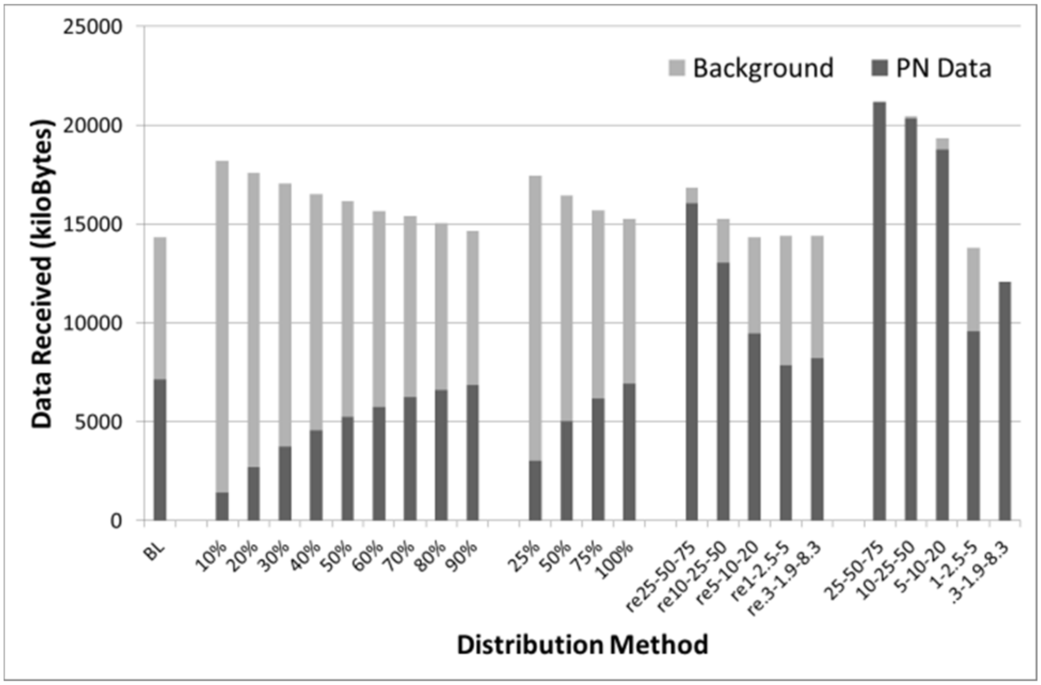


Figure 41. Total data received broken down by data type (200 OBU case).

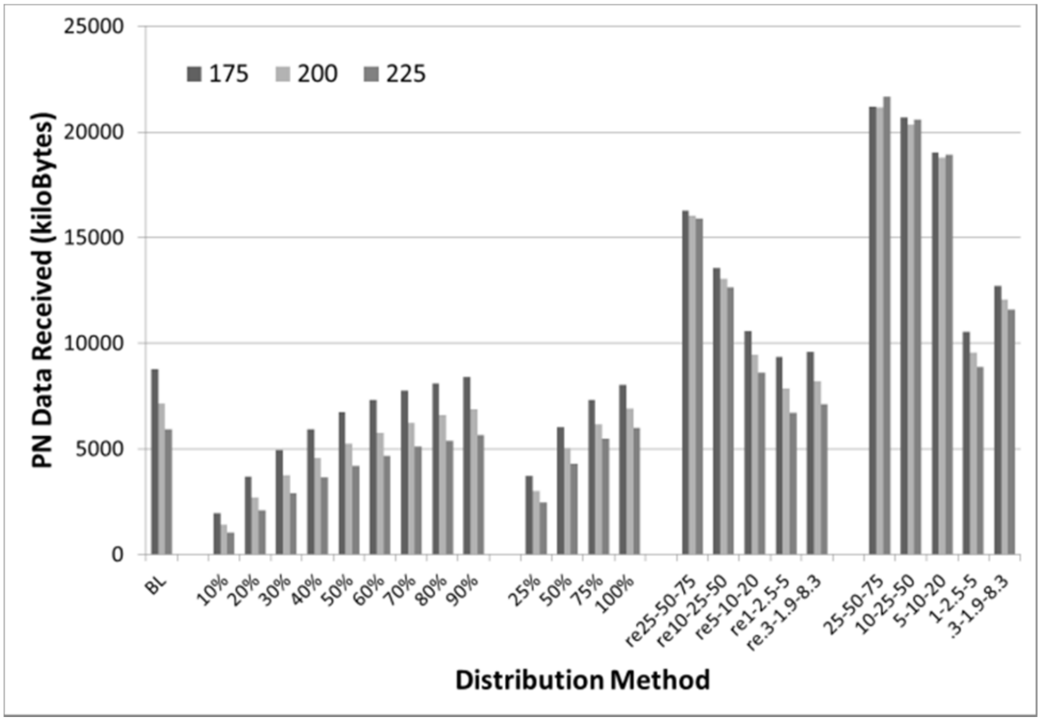


Figure 42. Total PN data received.

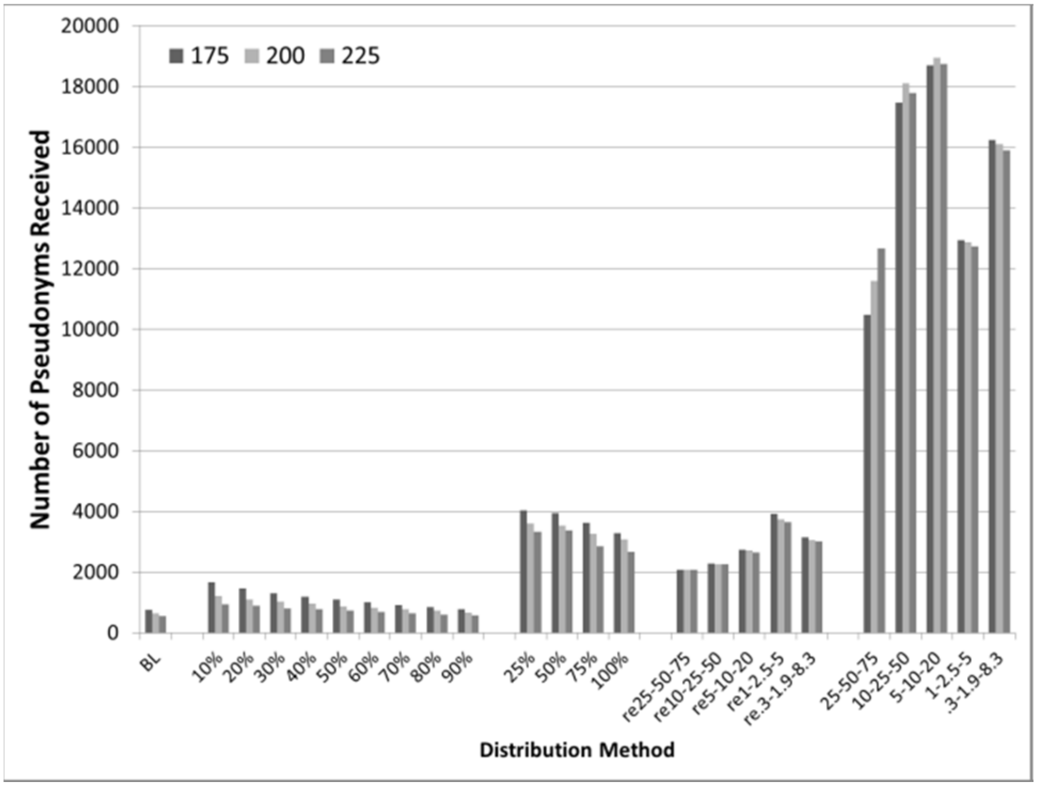


Figure 43. Maximum number of PNs received by a single OBU.

5.3.7 Distribution of PNs Distributed

As before, it is instructive to examine how the distribution of PNs affects vehicles with various levels of stored PNs. Figure 44 illustrates this point and shows that when all vehicles are equitably seeking PNs, as in the baseline case, they each receive a relatively equal amount. However, a relatively equal distribution of PNs may not be the goal when vehicles with very few PNs are present. In such circumstances, a method that discriminates the PNs based upon their need is better suited to deliver more PNs to these vehicles (and may result in the greatest number of PNs being delivered overall – but not the most overall data). Figure 44 also demonstrates that a strategy to how QoS might be implemented is an important factor. Setting the thresholds too liberally such that too many vehicles are transmitting at high priority results in fewer PNs being distributed. Setting the threshold too tightly can also have a deleterious effect.

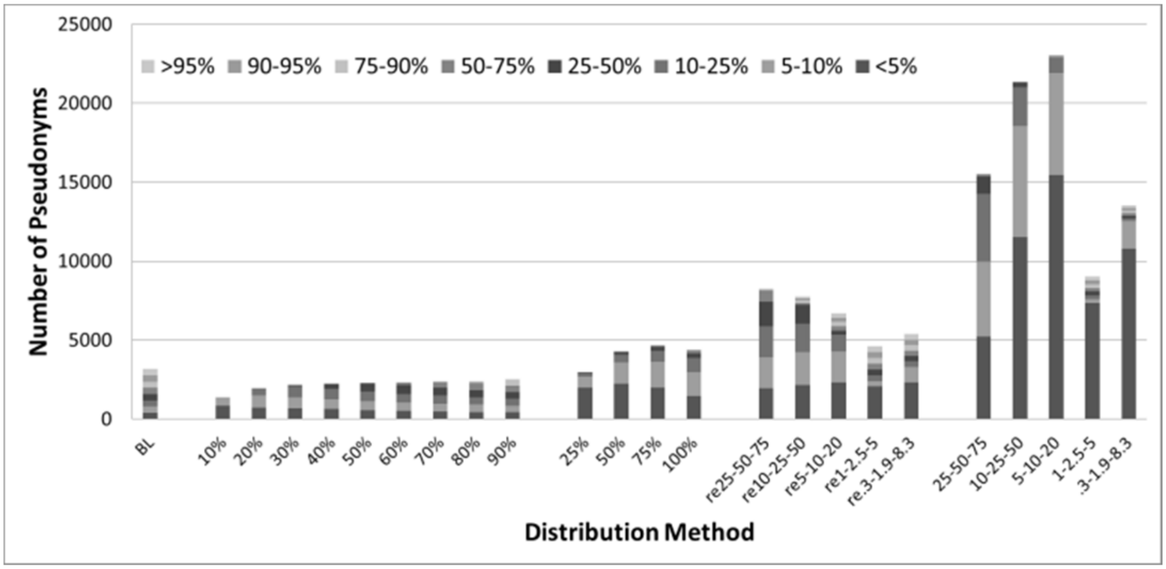


Figure 44. Breakdown of PNs received by OBU PN fill level (200 OBU case).

5.3.8 Section Summary

The results of this section further reinforce that an equitable distribution policy may not be “best” in providing PNs to vehicles. In 30 seconds with an RSU in two urban scenarios we simulated, the baseline method of granting equal priority to PN distribution resources only provided a maximum of 400 PNs (less than half a day’s) over 30 seconds in the 200 OBU case. On the other hand, once again we have shown that reducing the amount of requests for PNs positively effects the system performance. In this section we have extended this concept to show that the best performance in terms of PN distribution among the five techniques we examined was achieved with a QoS based PN distribution scheme. Such a method resulted in an increase of 25 – 800% compared to other methods. The implementation of QoS, or even a simpler method similar to QoS that requires no hardware support demonstrated substantial increases in PN distribution and hold much promise as being part of the solution to ensuring all OBU communication can be both secure and private.

5.4 Impact of PN Pre-computation and Subsequent Pre-distribution (including the Effects of OBU/RSU Cooperation and Various RSU Forwarding Techniques)

In this section, we examine the impact of having pseudonyms readily available for distribution when the vehicle requests them and how cooperation between OBUs and RSUs affects pre-distribution of these PNs. Extensive simulation was performed to estimate a reasonable delay to generate the pseudonyms. A generic roadway grid was then analyzed to estimate the performance of various pseudonym forwarding methods. Finally we considered three cases of vehicular traffic densities given probabilities of zero to one hundred percent that the pseudonyms are immediately available for transmission. From this work, we conclude that not having pseudonyms available for transmission adversely affects system performance and could be a good design enhancement for vehicular networks.

While considerable work has been performed in the area of routing within VANETs (see [131] for a summary) as well as the overhead associated with computing the Elliptic Curve Digital Signature Algorithm (ECDSA) in the functioning of VANETs [144], little research has been conducted on the unique problem of pseudonym distribution. This section examines the question of whether or not RSUs having PNs when an OBU requests them impacts the number of PNs a vehicle can obtain and if there is an impact, what is its extent. We conducted intensive simulations and validated our assumptions using the built-in OpenSSL benchmarking tool, MATLAB, and ns-3.

5.4.1 Assumptions Regarding the Refill Process

There are many ways for a vehicle to acquire PNs, such as through a physical USB connection or over a cellular or WiMax connection (requiring additional hardware and a service provider). Whether or not it is the primary means of PN distribution, it seems that vehicular networks should have this capability organically, especially when considering implementing regions to partition the global roadway infrastructure. While it may be possible for a vehicle to have a lifetime of PNs pre-installed for use within a given region, when it crosses logical borders within an authority or international borders (ex: driving from China to Russia), the ability to distribute PNs through the VANET becomes even more important.

It is assumed that when an OBU requires PNs, and upon receiving a beacon from an RSU advertising this service, it will transmit a request. When the RSU receives the request it will either transmit PNs to the OBU if it possesses them or acquire and then transmit them. As long as the OBU needs PNs and is in range of the RSU, it continues to receive them. Once it is out of range, the RSU can either do nothing or potentially forward the remaining PNs to other RSU(s).

In terms of communication range, we again used ns-3's Three-Log propagation loss model with parameter values from Section 4.5 as published in [106] to limit communication to 140 m for urban environments and 300 m for non-urban ones.

Pseudonym Availability

It is unlikely that every RSU would immediately have PNs for every vehicle. Given that the default service channel interval for dedicated short range communication (DSRC) is only approximately 46 ms [22], the delay in acquiring PNs to distribute is likely to impact how many PNs an OBU can acquire. One of the purposes of the research presented in this section is to provide insight into this issue.

Pseudonym Subsequent Pre-Computation

By pseudonym pre-computation we mean the process by which PNs are computed by RSUs prior to an OBU travelling within range of said RSU and requesting PNs. This is a measure of the greatest delay likely to be encountered when an OBU requests PNs from an RSU that does not presently have them and they are not in existence. It is possible, as discussed above, for PNs to be computed many different ways.

We are assuming for economy of scale reasoning that the PNs are computed in a distributed manner by the registration authorities (RAs) at the RSUs. (This method is considered in this work as opposed to a third party or via the OBUs themselves. The PNs may be signed by either the RSU acting as a RA whose certificate in turn is signed by the CA or could be transmitted to the CA for signing. While rogue RSUs may be deployed, we assume that the CA/RA periodically transmits a list of known good RSUs and only those are part of the RSUs that participate in PN forwarding. We have considered any infrastructure network delay this may introduce as negligible since we are focused here on pseudonym computation delay, however if this additional delay is not negligible, the results of this research become even more important because of the longer delays.) This means that computer hardware roughly equivalent to computers generally available in university labs would provide sufficient processing power to simulate our configuration. Thus in [145] we generated in C++ [146] on such computers certificates for the OBUs as defined in IEEE 1609.2 [26] using the nistp224 elliptic curve (in accordance with IEEE 1363 [147]) using OpenSSL in both 32 bit and 64 bit Windows using both the Microsoft Visual Studio 2010 Professional [148] and MinGW/gcc [149] compilers/integrated development environments.

Pseudonym Pre-distribution/Forwarding

By pseudonym pre-distribution/forwarding we mean the process by which PNs are forwarded to RSUs prior to an OBU travelling within range of said RSU and requesting PNs. We examined seven potential PN forwarding techniques for RSUs. Our goal is not to use all of these and identify when, but rather compare these various methods and glean insight from their relative performance. (1) The first is the GPS method in which the OBU communicates exactly which path it will follow. It is true that providing the network with one's path does impact privacy, but the general goal is to protect one's privacy from outside observers and such entities would still not be privy to this information. (2) Another option is a regional flood such that the remaining PNs are forwarded to all the other RSUs in a given region. (3) A third method involved forwarding the remaining PNs to all the adjacent RSUs – the first RSU encountered sectored by 45 degrees of arc. (4) The next method introduced involved forwarding the remaining PNs to the closest three RSUs. (5) The fifth method simply forwarded PNs to the two closest RSUs. (6) The sixth method used a fixed distance and forwarded the remaining PNs to all RSUs within that fixed distance. (7) The final method analyzed involved no forwarding.

The topology of the road network used in this phase of the research is provided in Figure 45 with the RSU locations indicated by diamonds.

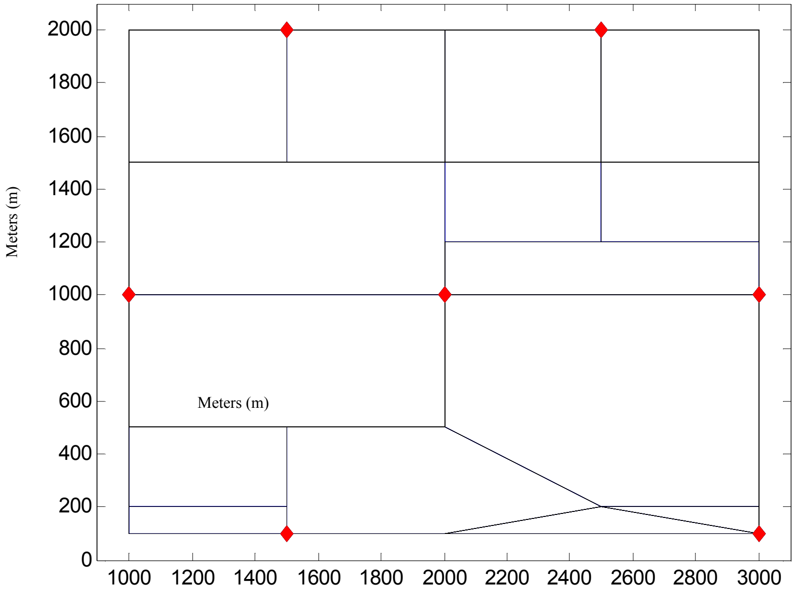


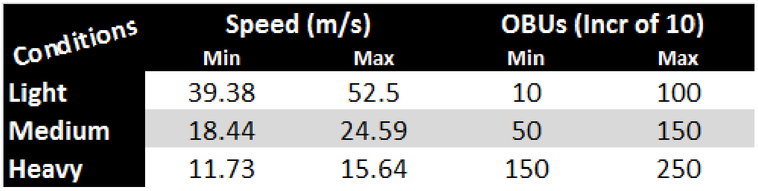
Figure 45. Road network and RSU placement used to determine probability RSUs had PNs when requested.

Traffic Conditions

Once the delay was calculated for the first PNs to be distributed assuming they were not pre-computed and the probability an OBU would encounter such a delay, the second phase of this research was to use ns-3 to simulate OBUs in the presence of multiple RSUs (using the probabilities of delays obtained in the first phase of the research) to measure the impact of the various delay probabilities. In real life, the traffic density will have a significant effect on VANET performance, with greater levels of congestion likely to have the worst impact.

For this purpose, three different scenarios were defined as summarized in Table 20. RSUs were simulated with the various densities of OBUs from the minimum to maximum values with each density simulated 30 times. The speeds were randomly selected for each vehicle from the minimum to maximum value and changed every ten seconds or 200 meters. In order to focus on the interaction of a set space, a multi-lane highway scenario was chosen with the vehicles equally distributed in each direction. A dense RSU scenario was examined that was 600 meters in extent with the RSUs placed 150 meters apart with the OBUs initially placed 10 m from each other with 10 m lane spacing. All simulations were run for 30 seconds of simulated time and the simulation communications range was the same as the previous two sections.

Table 20. Vehicular traffic density scenario configuration.



Conditions	Speed (m/s)		OBUs (Incr of 10)	
	Min	Max	Min	Max
Light	39.38	52.5	10	100
Medium	18.44	24.59	50	150
Heavy	11.73	15.64	150	250

5.4.2 Time Delay to Compute PNs

In order to estimate the amount of delay involved in order to compute PNs, the appropriate environment was coded and benchmarking was performed [145] using the built-in functionality of OpenSSL. The OpenSSL self-benchmarking functionality measures most cryptographic capabilities, but our focus was on the Elliptic Curve Cryptography and specifically the Elliptic Curve Signature Algorithm (ECDSA). Prior to calculating the PN generation times, we examined basic cryptographic functionality to compare performance among the various processors and compilers. These results, for both signing and verifying OBU certificates, are contained in Table 21. As can be seen, the best performance in terms of the maximum number of signing (creating) per second and the number of verifying (checking) per second operations was achieved using the 64 bit processor and the gcc compiler. As such, we limited future work to this best case scenario given VANETs are likely to implement similar hardware and software.

In terms of PN generation, we determined that 287 certificates could be generated per second. Given an example protocol of sending ~1000 bytes of PNs per packet (this value was selected to balance unnecessary overhead from smaller packets with larger packet sizes that increase the likelihood of collisions and other transmission errors), and that each PN is 153 bytes, this yields seven PNs being sent per service channel interval, and thus a creation delay of 24.4 ms. We conservatively estimate processing, queuing, transmission, and propagation delay to be 1.4 ms. Thus for the purposes of this simulation, we introduce a delay of 25.8 ms prior to an RSU replying to a PN request message if it is determined to not have the PNs in its memory.

Table 21. Basic cryptographic function benchmark results.

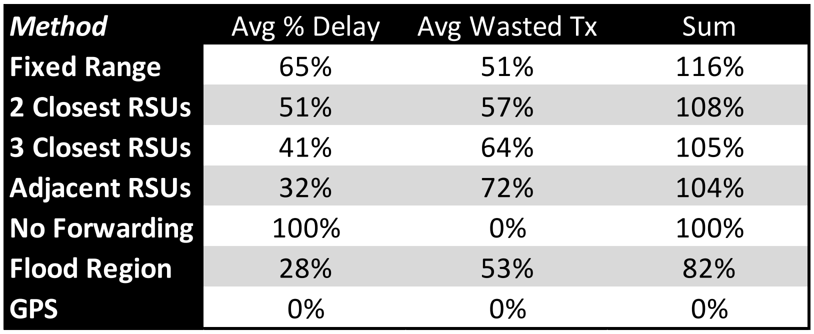
224 bit	w32-gcc47	w64-gcc47	w32-vc	w64-vc
sign/s	3618	6233.4	3635.9	4934.4
verify/s	767.4	1395.5	778.2	1069.9

5.4.3 RSU Pseudonym Forwarding

Given that a delay does exist should an RSU have to either generate PNs or request them from a Certificate Authority (CA) or a non-resident Registration Authority

(RA), minimizing the number of times an OBU requests PNs from an RSU that does not have them will improve the overall ability of the VANET to transmit PNs. We examined the seven forwarding techniques enumerated in Section 5.4.1 to determine the likelihood an OBU would encounter RSUs that would not possess them. These results are given in Table 22. The first column indicates the average percentage of the time for a given method that the PNs were not immediately available when the OBU encountered an RSU. The second column indicates the average percentage of PN forwarding transmissions to an RSU that either never encountered the OBU for which the PNs were generated or already had them from a previous forwarding incident

Table 22. PN forwarding method comparison.



Method	Avg % Delay	Avg Wasted Tx	Sum
Fixed Range	65%	51%	116%
2 Closest RSUs	51%	57%	108%
3 Closest RSUs	41%	64%	105%
Adjacent RSUs	32%	72%	104%
No Forwarding	100%	0%	100%
Flood Region	28%	53%	82%
GPS	0%	0%	0%

While these measurements are subject to variation due to topology and forwarding method configuration, our purpose was to evaluate the different techniques in order to justify the probability settings for the work in section 5.4.4. It is also difficult to determine which has a greater negative impact: time delay or wasted transmissions. Given the ephemeral nature of VANETs, it is most likely time delay is that one would like to minimize.

Figure 46 provides a visual comparison of the results of the seven methods. The GPS guided system that has the PNs pre-forwarded to just those RSUs has the expected delay and unnecessary transmissions of zero while flooding the region results in experiencing a delay roughly 25% of the time. Forwarding the PNs to the closest two or three RSUs resulted in RSUs not having PNs to distribute roughly 50% of the time. The fixed range method resulted in a delay 65% of the time. Given these results, we simulated the impact of PN availability on moving vehicles from 100% to 0% availability in 25% increments.

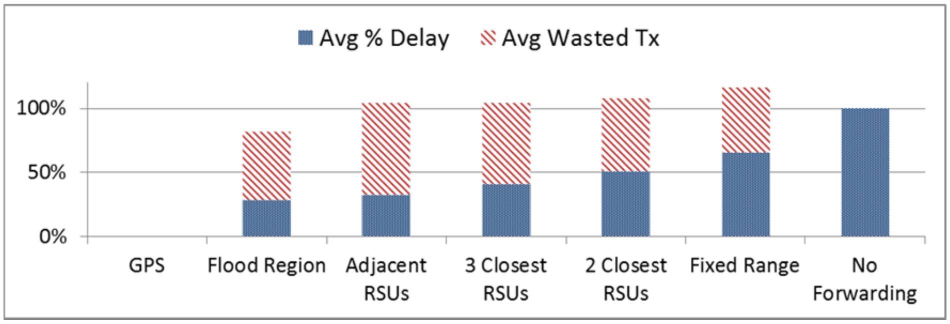


Figure 46. PN forwarding method comparison.

5.4.4 Impact of PN Availability

Having established a reasonable value to use for delay (25.8 ms) and reasonable values for the likelihood an OBU would encounter an RSU along its path that would not possess PNs to distribute to it (0%, 25%, 50%, 75%, and 100%), we proceeded to simulate in ns-3 for the vehicle speeds and densities listed in Table 20 and for both a dense and sparse RSU distribution to measure its impact. For the dense RSU case,

Figure 47 is an example of the results for all five delay scenarios under light traffic conditions. Figure 48and Figure 49 illustrate the medium and heavy traffic conditions. The behavior is similar for each scenario with increasing separation between the lines as one proceeds from light to heavy traffic.

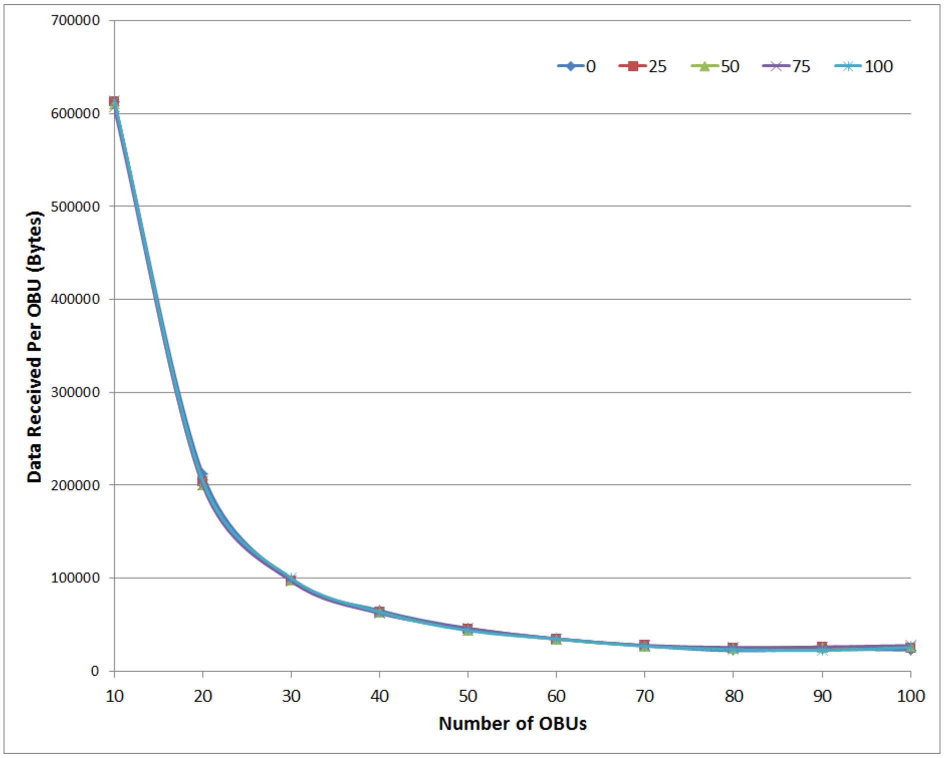


Figure 47. Simulation performance for light traffic scenario (dense RSU distribution).

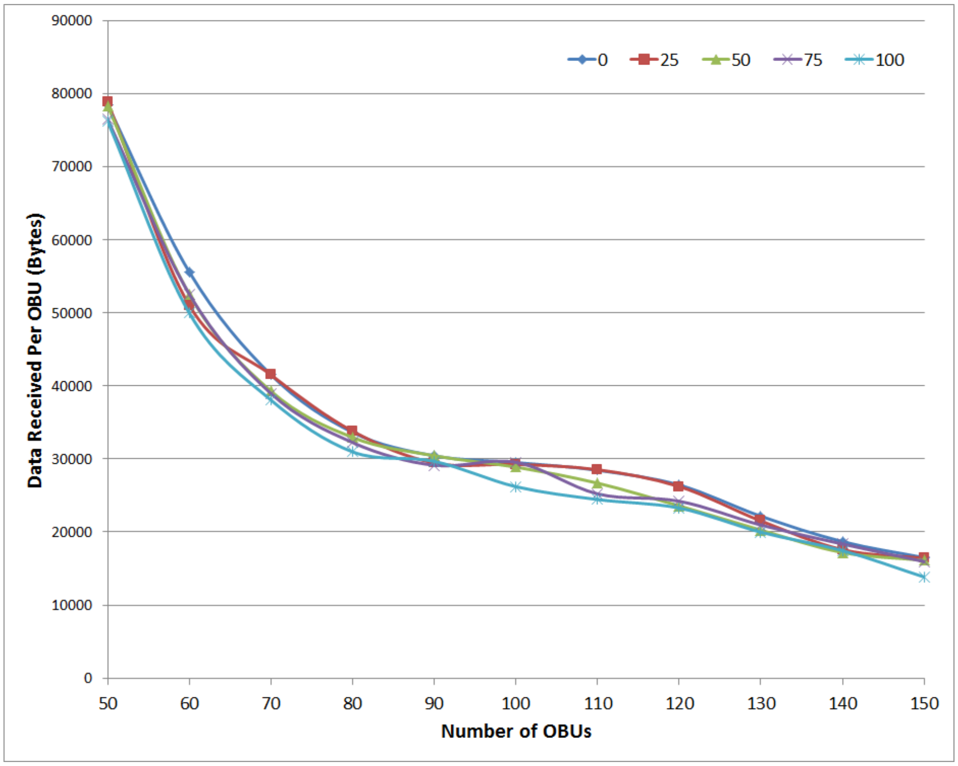


Figure 48. Simulation performance for medium traffic scenario (dense RSU distribution).

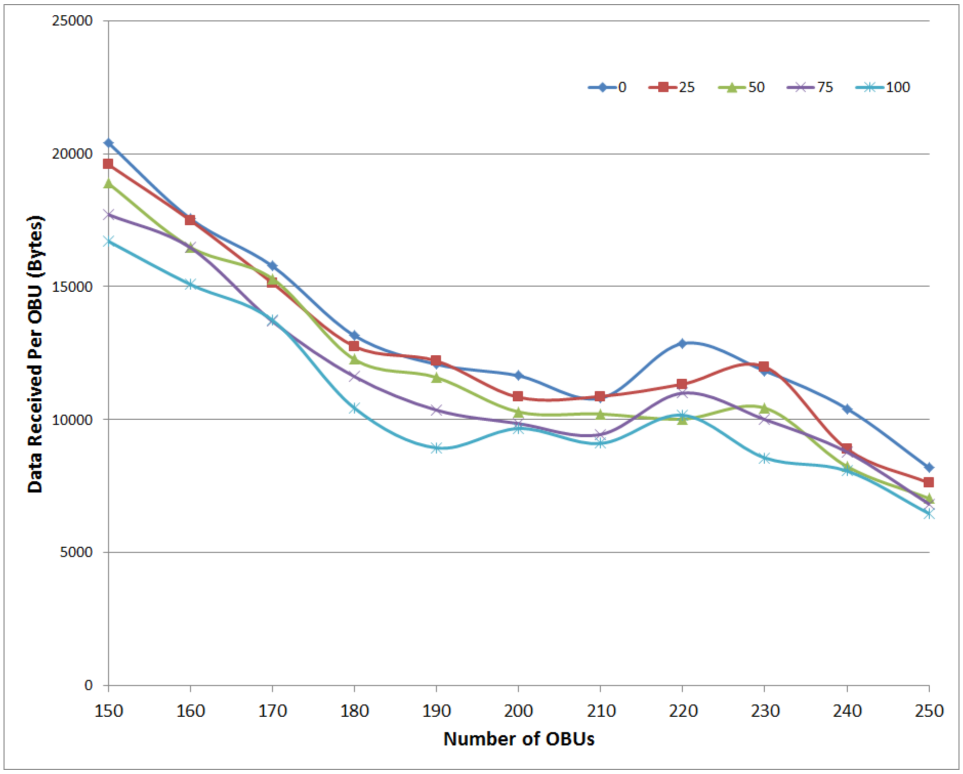
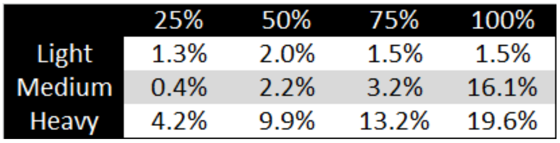


Figure 49. Simulation performance for heavy traffic scenario (dense RSU distribution).

When the numbers are more closely examined in tabular form (see Table 23), the impact can be more clearly seen. Here one sees that under light vehicular density conditions, OBUs receive about one to two percent less PNs than they would if the PNs were always available for distribution to the OBUs. However in the medium case, the impact of not having PNs to distribute when an OBU requests them increases considerably with each quintile. While it was expected that the heavy vehicular density case would have the greatest impact, its almost 20% magnitude was surprising. It would seem the added problem of congestion really limits how many packets a vehicle can acquire and exacerbates the impact of PNs not being available for immediate distribution.

Table 23. Average impact of PN availability for various traffic conditions



	25%	50%	75%	100%
Light	1.3%	2.0%	1.5%	1.5%
Medium	0.4%	2.2%	3.2%	16.1%
Heavy	4.2%	9.9%	13.2%	19.6%

5.4.5 Section Summary

In this section we have examined another aspect of PN distribution: the impact of having PNs available at RSUs for immediate delivery when an OBU contacts them and requests them. Through the use of OpenSSL and ns-3 simulation, we have demonstrated that PN pre-computation and pre-distribution is a worthwhile idea that can greatly assist in the PN distribution process, especially in congested environments. Doing so is likely to result in the distribution of anywhere from .4% to 19.6% more pseudonyms than a VANET infrastructure that does not support these under dense RSU distributions and a smaller performance enhancement in sparser RSU environments.

5.5 Comparison of WSMP to TCP

Throughout this work, the WAVE Short Message Protocol (a simplified version of the universal datagram protocol, UDP) was assumed to be used. An interesting thought was to see how using the Transmission Control Protocol (TCP) would affect performance. A simple scenario was established using the trace file discussed in Section 4.7.1 with 100 to 1000 OBUs in 100 OBU increments was conducted with eight RSUs positioned as in Figure 50.

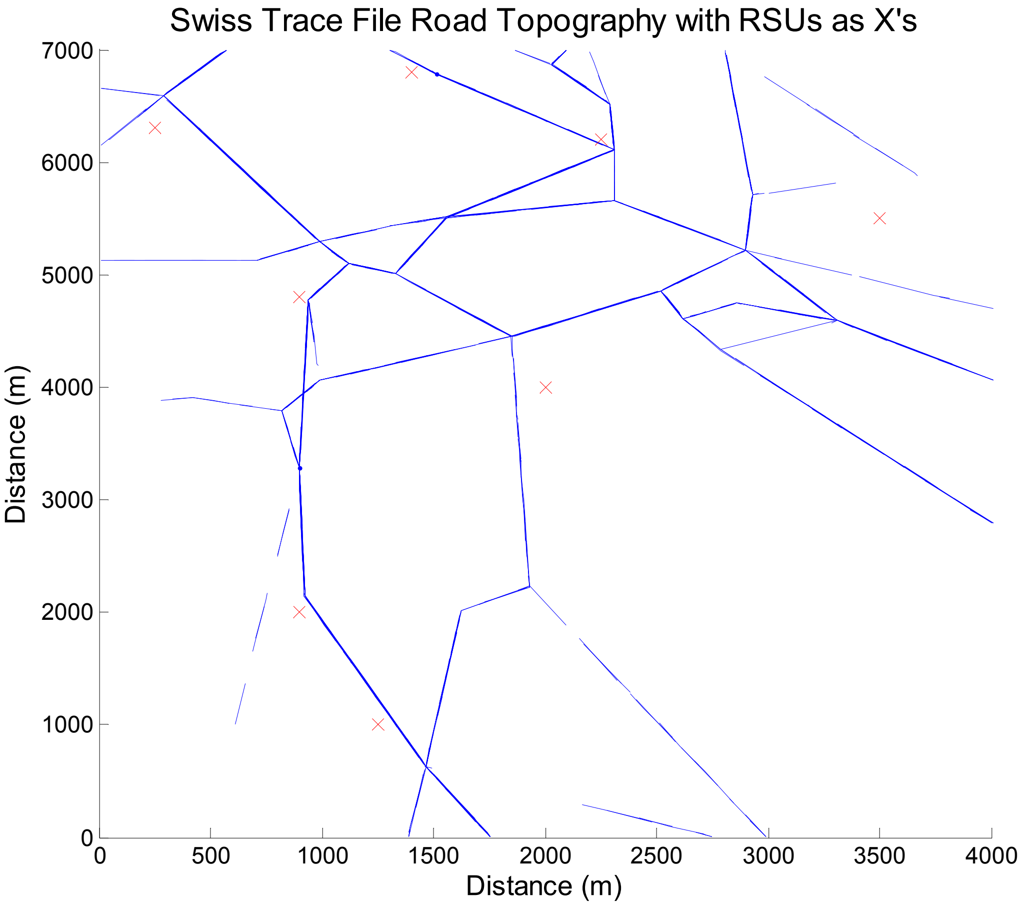


Figure 50. View of trace file roadway network and RSU positioning.

The results of this simulation run demonstrated rapidly that using TCP negatively affected performance and WSMP is a better selection. Overall, TCP distributed almost half of the amount of PN data compared with WSMP as shown in Figure 51 and Figure 52. The dramatic increase in data transmitted between 100 and 200 OBUs can be attributed to a larger number of OBUs more geographically disperse and able to communicate in a relatively congestion free radio environment.

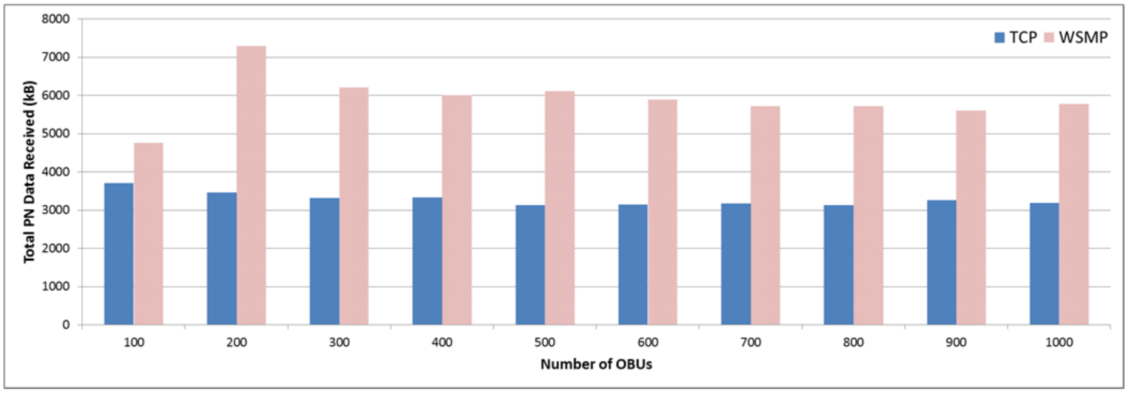


Figure 51. Total PN data received by all OBUs: TCP vs WSMP.

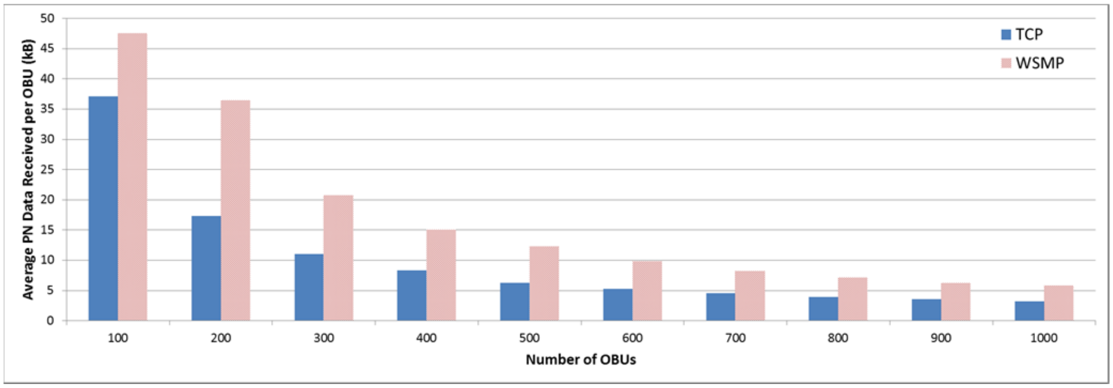


Figure 52. Average amount of PN data received per OBU: TCP vs WSMP.

CHAPTER 6

NEW COMPREHENSIVE METHOD OF PSEUDONYM DISTRIBUTION

6

6.1 Pseudonym Distribution Protocol (PNDP)

From the preceding sections we arrive at our final recommendations for a comprehensive PN distribution method. In Chapter 2 we reviewed the security, including privacy, considerations and requirements of VANETs. The implementation ideas found throughout the literature were discussed in Sections 3.1 through 3.3. Our designed VPKI was then developed and presented in Sections 3.4 through 3.7. Chapter 4 discussed our simulation configuration and the research we conducted in building a realistic propagation and fading loss model as well as discussed the use of actual vehicle position data provided as trace files for the most realistic large-scale mobility simulation. Our research presented in Section 5.2 demonstrated the value in restricting PN refill from all vehicles all the time (as proposed by some other authors) to only those in need. In Section 5.3 we show that using QoS (or if this will not be supported in VANETs, a light-weight equivalent protocol we designed that requires no hardware support) further improves the VPKI's ability to deliver PNs most effectively. Our PNDP protocol was further refined with the additional infrastructure support of PN pre-computation and subsequent pre-distribution as discussed in Section 5.4. Finally our intuitive decision to use WSMP over TCP was validated in Section 5.5.

In tying all of the lessons learned through this research, we believe we have demonstrated improved design features that result in an improved method for the comprehensive and universal distribution of pseudonyms in hybrid ephemeral vehicular networks.

6.2 Simulation Results

To see the difference between a baseline PN distribution method and the one above, we conducted a large scale simulation over 60 seconds for 1000 OBUs with the realistic mobility trace file and using the other simulation parameters of Chapter 4. As our baseline, we assumed that all OBUs requested PNs at all times, no QoS is implemented, and no PN pre-computation or forwarding was affected. For our protocol, we implemented QoS to suppress requests from OBUs with many PNs when others with few PNs were in the vicinity and we assumed GPS coordination between OBUs and RSUs was present to provide 100% effectiveness of PN pre-computation and forwarding. The size of the PN packet was 1071 bytes, representing seven PNs.

The final results of our protocol compared to the baseline protocol just described are illustrated in Figure 53. For 750, 1000, and 1250 OBU scenarios using the most realistic mobility trace model, PNDP outperforms a baseline method by an average of 36.1%. In all, we have conclusively shown that how PNs are distributed matters and that there are significant differences that will result based upon how a PN distribution protocol is designed. Our protocol transmitted a third more PNs and as such we believe it represents an excellent option for a unified approach to PN distribution in ephemeral vehicular networks.

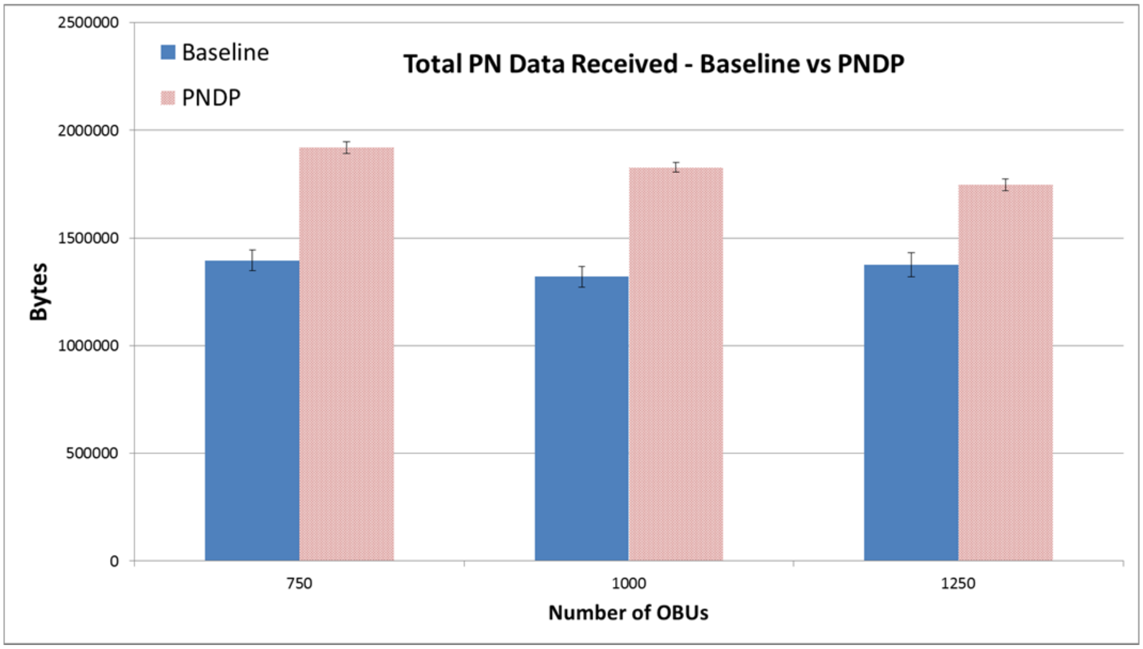


Figure 53. Final results of baseline PN distribution protocol vs. our PNDP.

6.3 Comparison of Results to Other Published Methods

At present, no other PN distribution technique's implementation details have been presented for a side-by-side comparison of performance. However throughout the literature there are other protocols that have been presented that meet aspects of the various requirements of VANETs and these, as well as our own, are as summarized in Table 24 [46-50, 65, 150-152].

Authentication and privacy refer to the definitions of Section 2.2. By centralization, we refer to whether the management is centrally organized or distributed with a preference for centralization given the need for government oversight of vehicular networks. Sparsity refers to whether the method can work under conditions with few vehicles, little infrastructure, and minimal contact. For example, a method can handle sparsity if two vehicles who have never seen each other and with no external infrastructure present can securely communicate. A Dynamic trust model is one in which the system can adjust to change – such as a car experiencing electrical failures that result in sending false information. Our method relies on CRLs and the renewal process to achieve dynamism. Given the large scale of VANETs, the need for any system that provides security to scale is necessary. Our method achieves this through RAs and regions. Confidence refers to how much trust one can put in the system itself. Our method is grounded in the principles of public key infrastructure and is equally secure. Thus communications can be comparatively trusted if the sender's certificate has been signed by the CA. Finally, robustness is a measure of how a trust system can withhold attacks, such as a Sybil Attack. Reputation based systems are quite vulnerable to these, but PKIs when properly implemented greatly reduce the ability for identity fraud and are inherently secure.

Table 24. Comparison of PNDP to other trust approaches within VANETs.

	Authentication	Privacy	Centralization	Sparsity	Dynamic	Scalable	Confidence	Robust
Benin	x	x	x	x	x	x	x	x
Chen	x			x	x	x	x	
Dotzer		x			x			
Gerlach	x	x	x	x	x		x	
Golle	x	x		x				x
Ma	x	x	x	x			x	x
Minhas	x			x	x	x	x	
Patwardhan	x			x	x			
Raya	x				x		x	

CHAPTER 7

CONCLUSION

7.1 Conclusion

The purpose of this research was to devise a unified method for the distribution of pseudonyms in ephemeral hybrid vehicular networks. Our research has resulted in the development of a pseudonym distribution protocol that takes into consideration the many relevant factors without compromising the security or privacy of pseudonym users. Our approach is scalable, adaptive, and bandwidth efficient and should prove to help pave the way to networked vehicles. The ultimate result we hope this research contributes to is safer roads with fewer vehicle accidents, injuries, and deaths.

7.2 Future Work

This work provides insight to the problem of pseudonym distribution through the use of simulation. The next step would be to further validate these results through the use of either full scale vehicles or micro-scale models. In this way VANETs can be validated as providers of augmented information to drivers and vehicle electronic control systems, such as dynamic laser cruise control.

Furthermore, with adequate solutions for both PN distribution and revocation now attained, implementing a VPKI complete with CAs, RAs, PNs, and OBUs to gain insight in the interaction of the total VPKI system is possible. In doing so, additional insights are likely to be gained and additional ideas on how to improve a VPKI would be generated.

Finally, with autonomous vehicles becoming a reality and now legal in both Nevada and California, integrating networked vehicles with autonomous vehicles is bound to be the future of independent small group transportation. Ultimately we predict that the first major Segway into our roadways will be the replacement of High Occupancy Vehicle (HOV) lanes with Networked-Autonomous Vehicle (NAV) lanes that will provide for safer, faster, and more environmentally friendly travel. Individual NAVs will join in close proximity in building a customized technological mass transit system that, combined with improvements in alternative energy, will bring to the market tremendous gains in freedom of movement and one day achieve the goals of the Intelligent Transportation System conceived over 40 years ago. The future is both promising and exciting and we believe that this work is one of many enablers to bringing it to fruition.

REFERENCES

[1] S. McCann and A. Ashley. (2010, 11/29/10). *Official IEEE 802.11 Working Group Project Timelines - 2010-11-12*. Available: http://www.ieee802.org/11/Reports/802.11_Timelines.htm

[2] "To New Horizons," ed: General Motors, 1939.

[3] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Identifier Allocations," *IEEE P1609.12-2012,* pp. 1-20, 2012.

[4] NHTSA, "2009 Traffic Safety Facts Data Summary Booklet," *DOT HS 811 401,* 2011.

[5] NHTSA, "2010 Motor Vehicle Crashes: Overview," *DOT HS 811 552,* 2012.

[6] NHTSA, "Traffic Safety Facts 2008 Data Rural/Urban Comparison," *DOT HS 811 164,* 2010.

[7] NHTSA, "Geospatial Analysis of Rural Motor VehicleTraffic Fatalities," *DOT HS 811 196,* 2009.

[8] S. Roglinger and C. Facchi, "How Can Car2C-Communication Improve Road Safety," Ingolstadt, 2009.

[9] S. E. Shladover, "ROADWAY AUTOMATION TECHNOLOGY - RESEARCH NEEDS," *Transportation Research Record* pp. 158-167, 1990.

[10] USDOT, "ITS Strategic Research Plan, 2010-2014 : Executive Summary," 2010.

[11] H. Hartenstein and K. P. Laberteaux. (2008, June) A Tutorial Survey on Vehicular Ad Hoc Networks. *IEEE Communications Magazine*. 164-171.

[12] D. A. Rosen*, et al.*, "An electronic route-guidance system for highway vehicles," *Vehicular Technology, IEEE Transactions on,* vol. 19, pp. 143-152, 1970.

[13] H. Hartenstein and K. Laberteaux, *VANET Vehicular Applications and Inter-Networking Technologies*, 1 ed. West Sussex, United Kingdom: John Wiley & Sons Ltd, 2010.

[14] "FCC ALLOCATES SPECTRUM IN 5.9 GHz RANGE FOR INTELLIGENT TRANSPORTATION SYSTEMS USES," Office of Engineering and Technology, Washington, DC ET 99-5, 1999.

[15] (12/1/2010). *IntelliDrive*. Available: http://www.intellidriveusa.org/

[16] USDOT. (2012, 10/11/12). *Safety Pilot Program Overview*. Available: http://www.its.dot.gov/safety_pilot/index.htm

[17] K. Matheus*, et al.*, "Car-to-car communication - market introduction and success factors," in *ITS 2005: 5th European Congress and Exhibition on Intelligent Transport Systems and Services*, 2005.

[18] S. Eichler, "Performance evaluation of the IEEE 802.11p WAVE communication standard," in *IEEE 66th Vehicular Technology Conference, 2007*, 2007, pp. 2199-2203.

[19] M. Torrent-Moreno*, et al.*, "Distributed Fair Transmit Power Adjustment for Vehicular Ad Hoc Networks," in *Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on*, 2006, pp. 479-488.

[20] IEEE, "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009),* pp. 1-51, 2010.

[21] IEEE, "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," in *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, ed, 2007.

[22] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Multi-channel Operation," *IEEE Std 1609.4-2010 (Revision of IEEE Std 1609.4-2006),* pp. 1-89, 2011.

[23] "IEEE Draft Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture," *IEEE P1609.0/D5, September 2012,* pp. 1-74, 2012.

[24] T. K. Mak*, et al.*, "A multi-channel VANET providing concurrent safety and commercial services," presented at the Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, Cologne, Germany, 2005.

[25] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services," *IEEE Std 1609.3-2010 (Revision of IEEE Std 1609.3-2007),* pp. 1-144, 2010.

[26] IEEE, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages," in *IEEE Std 1609.2-2006*, ed, 2006.

[27] M. Raya and J. P. Hubaux, "Security Aspects of Inter-Vehicle Communications," in *STRC 2005 (Swiss Transport Research Conference)*, 2005.

[28] IEEE, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Resource Manager," in *IEEE Std 1609.1-2006*, ed, 2006.

[29] "IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-- Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)," *IEEE Std 1609.11-2010,* pp. 1-62, 2011.

[30] I. D. W. Group. (2002, 12/6/2010). DSRC 5.9 GHz Tutorial Presentation. [Presentation]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html

[31] NHTSA, "Vehicle Safety Communications Project Task 3 Final Report Identify Intelligent Vehicle Safety Applications Enabled by DSRC," *DOT HS 809 859,* 2005.

[32] W. Xiang*, et al.*, "Introduction and Preliminary Experimental Results of Wireless Access for Vehicular Environments (WAVE) Systems," in *Mobile and Ubiquitous Systems - Workshops, 2006. 3rd Annual International Conference on*, 2006.

[33] Q. Xu*, et al.*, "Vehicle-to-vehicle safety messaging in DSRC," presented at the Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, Philadelphia, PA, USA, 2004.

[34] H. Wu*, et al.*, "Analytical models for information propagation in vehicle-to-vehicle networks," in *IEEE 60th Vehicular Technology Conference*, 2004, pp. 4548-4552.

[35] F. Kargl*, et al.* (2008) Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges. *IEEE Communications Magazine*. 110-118.

[36] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks,* vol. 15, pp. 39-68, 2007.

[37] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks," in *HotNets-IV*, College Park, Maryland, 2005.

[38] C. Solomon. (2010, 12/6/2010). *Cars that last a million miles*. Available: http://articles.moneycentral.msn.com/SavingandDebt/SaveonaCar/CarsThatLastAMillionMiles.aspx

[39] P. Papadimitratos*, et al.* (2008, November) Secure Vehicular Communication Systems: Design and Architecture. *IEEE Communications Magazine*. 100-109.

[40] Q. Yi and N. Moayeri, "Design of Secure and Application-Oriented VANETs," in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, 2008, pp. 2794-2799.

[41] A. A. Carter and J. Chang, "Using Dedicated Short Range Communications for Vehicle Safety Applications - The Next Generation of Collision Avoidance," 09-0330, 2009.

[42] F. Doetzer, "Privacy Issues in Vehicular Ad Hoc Networks," presented at the Workshop on Privacy Enhancing Technologies, Cavtat, Croatia, 2005.

[43] M. Raya*, et al.*, "Securing Vehicular Communications," *IEEE Wireless Communications,* vol. 13, pp. 8-15, 2006.

[44] S. Eichler, "A security architecture concept for vehicular network nodes," in *Information, Communications & Signal Processing, 2007 6th International Conference on*, 2007.

[45] V. Paruchuri, "Inter-vehicular communications: Security and reliability issues," in *ICT Convergence (ICTC), 2011 International Conference on*, 2011, pp. 737-741.

[46] F. Dotzer*, et al.*, "VARS: a vehicle ad-hoc network reputation system," in *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*, 2005, pp. 454-456.

[47] P. Golle*, et al.*, "Detecting and correcting malicious data in VANETs," presented at the Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, Philadelphia, PA, USA, 2004.

[48] C. Chen*, et al.*, "A Trust Modeling Framework for Message Propagation and Evaluation in VANETs," in *Information Technology Convergence and Services (ITCS), 2010 2nd International Conference on*, 2010.

[49] M. Gerlach, "Trust for Vehicular Applications," in *Autonomous Decentralized Systems, 2007. ISADS '07. Eighth International Symposium on*, 2007, pp. 295-304.

[50] A. Patwardhan*, et al.*, "A Data Intensive Reputation Management Scheme for Vehicular Ad Hoc Networks," in *Mobile and Ubiquitous Systems: Networking & Services, 2006 Third Annual International Conference on*, 2006.

[51] Q. Ding*, et al.*, "Reputation-based trust model in Vehicular Ad Hoc Networks," in *Wireless Communications and Signal Processing (WCSP), 2010 International Conference on*, 2010.

[52] L. Zhang*, et al.*, "A Scalable Robust Authentication Protocol For Secure Vehicular Communications," *Vehicular Technology, IEEE Transactions on,* 2009.

[53] P. Kamat*, et al.*, "Secure, pseudonymous, and auditable communication in vehicular ad hoc networks," *Security and Communication Networks,* vol. 1, pp. 233-244, 2008.

[54] L. Xiaodong*, et al.*, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," *Vehicular Technology, IEEE Transactions on,* vol. 56, pp. 3442-3456, 2007.

[55] G. Calandriello*, et al.*, "Efficient and robust pseudonymous authentication in VANET," presented at the Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks, Montreal, Quebec, Canada, 2007.

[56] Y. C. Hu and K. Laberteaux, "Strong VANET Security on a Budget," in *Proceedings of the 4th Annual Conference on Embedded Security in Cars (ESCAR 2006)*, Berlin, Germany, 2006.

[57] M. Akhlaq*, et al.*, "Empowered Certification Authority in VANETs," in *Advanced Information Networking and Applications Workshops, 2009. WAINA '09. International Conference on*, 2009, pp. 181-186.

[58] C. Tat Wing*, et al.*, "Security and Privacy Issues for Inter-vehicle Communications in VANETs," in *Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 2009. SECON Workshops '09. 6th Annual IEEE Communications Society Conference on*, 2009.

[59] J. R. Vacca, *Public Key Infrastructure: Building Trusted Applications and Web Services.* : Auerbach Publications, 2004.

[60] D. Cooper*, et al.*, "RFC5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," ed: RFC Editor, 2008.

[61] NIST, "FIPS 186-2 DIGITAL SIGNATURE STANDARD (DSS)," ed: National Institute of Standards and Technology, 2000.

[62] A. Studer*, et al.*, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON '09. 6th Annual IEEE Communications Society Conference on*, 2009.

[63] J. J. Haas*, et al.*, "Design and analysis of a lightweight certificate revocation mechanism for VANET," presented at the Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking, Beijing, China, 2009.

[64] J. Liao and J. Li, "Effectively Changing Pseudonyms for Privacy Protection in VANETs," in *Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on*, 2009, pp. 648-652.

[65] Z. Ma*, et al.*, "Pseudonym-on-demand: a new pseudonym refill strategy for vehicular communications," in *IEEE 68th Vehicular Technology Conference*, 2008.

[66] S. Eichler*, et al.*, "Car-to-Car Communication," in *VDE-Kongress - Innovations for Europe*, Aachen, 2006.

[67] M. E. Nowatkowski and H. L. Owen, "Certificate revocation list distribution in VANETs using Most Pieces Broadcast," in *IEEE SoutheastCon 2010 (SoutheastCon), Proceedings of the*, 2010, pp. 238-241.

[68] J. P. Hubaux*, et al.*, "The security and privacy of smart vehicles," *Security & Privacy, IEEE,* vol. 2, pp. 49-55, 2004.

[69] J. Benin*, et al.*, "Framework to Support Per Second Shifts of Pseudonyms in Regional VANETs," presented at the Vehicular Technology Conference, Ottawa, Ontario, Canada, 2010.

[70] J. J. Haas*, et al.*, "The impact of key assignment on VANET privacy," *SECURITY AND COMMUNICATION NETWORKS,* 2009.

[71] E. Schoch*, et al.* (2007, Impact of pseudonym changes on geographic routing in VANETs. *Lect Notes Comput Sci (LNCS),* 43-57.

[72] M. Raya and J.-P. Hubaux, "The Security of Vehicular Ad Hoc Networks," presented at the Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, VA, USA, 2005.

[73] J. Freudiger*, et al.*, "Mix-zones for location privacy in vehicular networks," presented at the WiN-ITS 2007, Vancouver, British Columbia, Canada, 2007.

[74] L. Buttyan*, et al.*, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in Vanets," in *3rd Euro. Wksp. Sec. and Privacy in Ad Hoc and Sensor Networks*, 2007, pp. 129-41.

[75] K. Sampigethaya*, et al.*, "CARAVAN: Providing Location Privacy for VANET," in *Workshop on Embedded Security in Cars (ESCAR)*, 2005.

[76] S. Eichler, "Strategies for Pseudonym Changes in Vehicular Ad Hoc Networks depending on Node Mobility," in *IEEE Intelligent Vehicles Symposium (IV)*, Istanbul, Turkey, 2007.

[77] S. Balfe*, et al.*, "Challenges for Trusted Computing," Royal Holloway, University of London, London, 2008.

[78] J. McCallum. (9/26/12). *Disk Drive Storage Price Decreasing with Time (1955-2012)*. Available: http://www.jcmit.com/disk2012.htm

[79] J. Y. Choi*, et al.*, "Balancing auditability and privacy in vehicular networks," presented at the Proceedings of the 1st ACM international workshop on Quality of service; security in wireless and mobile networks, Montreal, Quebec, Canada, 2005.

[80] M. Gerlach and F. Guttler, "Privacy in VANETs using Changing Pseudonyms - Ideal and Real," in *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, 2007, pp. 2521-2525.

[81] B. K. Chaurasia and S. Verma, "Maximizing anonymity of a vehicle through pseudonym updation," presented at the Proceedings of the 4th Annual International Conference on Wireless Internet, Maui, Hawaii, 2008.

[82] M. Nowatkowski*, et al.*, "Cooperative Certificate Revocation List Distribution Methods in VANETs," presented at the AdHocNets, Niagara Falls, Ontario, Canada, 2009.

[83] J. J. Haas*, et al.*, "Efficient Certificate Revocation List Organization and Distribution," *Selected Areas in Communications, IEEE Journal on,* vol. 29, pp. 595-604, 2011.

[84] M. Nowatkowski*, et al.*, "The Effects of Limited Lifetime Pseudonyms on Certificate Revocation List Size in VANETs," presented at the IEEE SoutheastCon, Charlotte, NC, 2010.

[85] L. Bisheng*, et al.*, "Probabilistic Isolation of Malicious Vehicles in Pseudonym Changing VANETs," in *Computer and Information Technology, 2007. CIT 2007. 7th IEEE International Conference on*, 2007, pp. 967-972.

[86] T. Moore*, et al.*, "Fast Exclusion of Errant Devices From Vehicular Networks," in *IEEE SECON*, San Fransisco, 2008.

[87] E. Barker*, et al.*, "Recommendation for Key Management – Part 1: General (Revised)," *NIST Special Publication 800-57,* 2007.

[88] B. Bellur, "Certificate assignment strategies for a PKI-based security architecture in a vehicular network," presented at the IEEE Global Telecommunications Conference, New Orleans, LA, 2008.

[89] C. Doyle, "Statutes of Limitation in Federal Criminal Cases: An Overview," *Congressional Research Service,* vol. RL31253, 4/9/2007.

[90] J. Benin*, et al.*, "Unified pseudonym distribution in VANETs," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2010 IEEE 6th International Conference on*, 2010, pp. 529-533.

[91] D. Huang, "Pseudonym-based cryptography for anonymous communications in mobile ad hoc networks," *International Journal of Security and Networks,* vol. 2, pp. 272-283, 2007.

[92] C. Lai*, et al.*, "A secure anonymous key mechanism for privacy protection in VANET," in *Intelligent Transport Systems Telecommunications,(ITST),2009 9th International Conference on*, 2009, pp. 635-640.

[93] B. K. Chaurasia*, et al.*, "Maximizing anonymity of a vehicle," in *Wireless Communication and Sensor Networks, 2008. WCSN 2008. Fourth International Conference on*, 2008, pp. 95-98.

[94] B. K. Chaurasia*, et al.*, "Pseudonym Based Mechanism for Sustaining Privacy in VANETs," in *Computational Intelligence, Communication Systems and Networks, 2009. CICSYN '09. First International Conference on*, 2009, pp. 420-425.

[95] (11/1/2012). *The ns-3 network simulator*. Available: http://www.nsnam.org/index.html

[96] M. E. Nowatkowski*, et al.*, "The Effects of Limited Lifetime Pseudonyms on Certificate Revocation List Size in VANETS," in *IEEE SoutheastCon 2010 (SoutheastCon), Proceedings of the*, 2010, pp. 380-383.

[97] IEEE, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation," in *IEEE Std 1609.4-2006*, ed, 2006.

[98] I. William J. Palm, *Introduction to Matlab 7 for Engineers*. New York, NY: McGraw Hill, 2005.

[99] J. Banks*, et al.*, *Discrete-Event System Simulation*, Fifth ed.: Prentice-Hall, 2009.

[100] (10/9/2012). *REAL 5.0 Overview*. Available: http://www.cs.cornell.edu/skeshav/real/overview.html

[101] (10/9/2012). *Network Simulator for Windows*. Available: http://ce.sharif.edu/~m_amiri/project/networksimulator1/index.htm

[102] (10/9/2012). *The Network Simulator - ns-2*. Available: http://www.isi.edu/nsnam/ns/

[103] G. Riley. (10/9/2012). Network Simulation with ns-3. Available: www.nsnam.org/tutorials/SpringSim-2010-Riley.pptx

[104] GNU. (2012, 11/1/2012). *The ns-3 network simulator*. Available: http://www.nsnam.org/index.html

[105] M. Nowatkowski, "Certificate revocation list distribution in vehicular ad hoc networks," Ph.D., Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, 2010.

[106] J. Benin*, et al.*, "Vehicular Network Simulation Propagation Loss Model Parameter Standardization in ns-3 and Beyond," presented at the IEEE SoutheastCon 2012, Orlando, FL, 2012.

[107] (6/29/2011). *ns3::YansWifiPhy Class Reference*. Available: http://www.nsnam.org/doxygen/classns3_1_1_yans_wifi_phy.html

[108] (2011, 2/23/2011). *ns3::PropagationLossModel Class Reference*. Available: http://www.nsnam.org/doxygen-release/classns3_1_1_propagation_loss_model.html#_details

[109] (1999, 2/23/2011). *COST 231*. Available: http://www.lx.it.pt/cost231/

[110] (2/23/2011). *Deterministic Two Ray Model*. Available: http://www.awe-communications.com/Propagation/Rural/DTR/index.htm

[111] Z. Yahong Rosa and X. Chengshan, "Simulation models with correct statistical properties for Rayleigh fading channels," *Communications, IEEE Transactions on,* vol. 51, pp. 920-928, 2003.

[112] D. Jiang*, et al.*, "Optimal data rate selection for vehicle safety communications," presented at the Proceedings of the fifth ACM international workshop on VehiculAr InterNETworking, San Francisco, California, USA, 2008.

[113] M. Torrent-Moreno, "Inter-Vehicle Communications: Assessing Information Dissemination Under Safety Constraints," in *Wireless on Demand Network Systems and Services, 2007. WONS '07. Fourth Annual Conference on*, 2007, pp. 59-64.

[114] Y. Fan and S. Biswas, "A Self-Organizing MAC Protocol for DSRC based Vehicular Ad Hoc Networks," in *Distributed Computing Systems Workshops, 2007. ICDCSW '07. 27th International Conference on*, 2007, pp. 88-93.

[115] V. Kukshya and H. Krishnan, "Experimental Measurements and Modeling for Vehicle-to-Vehicle Dedicated Short Range Communication (DSRC) Wireless Channels," in *IEEE 64th Vehicular Technology Conference*, 2006.

[116] C. Lin*, et al.*, "Mobile Vehicle-to-Vehicle Narrow-Band Channel Measurement and Characterization of the 5.9 GHz Dedicated Short Range Communication (DSRC) Frequency Band," *Selected Areas in Communications, IEEE Journal on,* vol. 25, pp. 1501-1516, 2007.

[117] F. Bai*, et al.*, "Toward understanding characteristics of dedicated short range communications (DSRC) from a perspective of vehicular network engineers," presented at the Proceedings of the sixteenth annual international conference on Mobile computing and networking, Chicago, Illinois, USA, 2010.

[118] K. Nagel. (2006, 10/10/2012). *Realistic Vehicular Traces*. Available: http://www.lst.inf.ethz.ch/research/ad-hoc/car-traces/index.html#paper

[119] V. Naumov*, et al.*, "An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces," presented at the Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing, Florence, Italy, 2006.

[120] A. M. Law, "Statistical analysis of simulation output data: the practical state of the art," presented at the Proceedings of the 39th conference on Winter simulation: 40 years! The best is yet to come, Washington D.C., 2007.

[121] A. M. Law and W. D. Kelton, *Simulation Modeling and Analysis*, Third ed.: McGraw Hill, 2000.

[122] J. Banks, Ed., *Handbook of Simulation*. John Wiley & Sons, Inc., 1998.

[123] J. Banks*, et al.*, *Discrete-Event System Simulation*, Second ed.: Prentice-Hall, 1999.

[124] (11/1/2012). *ns-3 Manual*. Available: http://www.nsnam.org/docs/manual.html

[125] (Georgia Institute of Technology, 10/11/2012). *PACE A Partnership for an Advanced Computing Environment*. Available: http://www.pace.gatech.edu/

[126] S. Cherry. (9/29/11). *The Car as Informant*. Available: http://spectrum.ieee.org/podcast/telecom/security/the-car-as-informant

[127] L. Jie*, et al.*, "A Mobile Infrastructure Based VANET Routing Protocol in the Urban Environment," in *Communications and Mobile Computing (CMC), 2010 International Conference on*, 2010, pp. 432-437.

[128] L. Jeng-Wei*, et al.*, "A hybrid traffic geographic routing with cooperative traffic information collection scheme in VANET," in *Advanced Communication Technology (ICACT), 2011 13th International Conference on*, 2011, pp. 1496-1501.

[129] H. Song*, et al.*, "P2P Computing in Design of VANET Routing Protocol," in *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*, 2007, pp. 1502-1507.

[130] T. Atechian*, et al.*, "CoFFee: Cooperative and inFrastructure-Free peer-to-peer system for VANET," in *Intelligent Transport Systems Telecommunications,(ITST),2009 9th International Conference on*, 2009, pp. 510-515.

[131] P. Rani*, et al.*, "Performance Comparison of VANET Routing Protocols," in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on*, 2011.

[132] Z. Wang and M. Hassan, "How much of dsrc is available for non-safety use?," presented at the Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking, San Francisco, California, USA, 2008.

[133] "World Population Prospects: The 2006 Revision and World Urbanization Prospects: The 2007 Revision," *Population Division of the Department of Economic and Social Affairs of the United Nations Secretariat,* 2007.

[134] A. Downs, "Traffic: Why It's Getting Worse, What Government Can Do," Brookings Institute, Washington, DC, 2004.

[135] "Field District 7 ATR Traffic Data Report Annual Summary," *State of Georgia,* p. 53, 2007.

[136] M. Raya*, et al.*, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE Journal on Selected Areas in Communications,* vol. 25, 2007.

[137] IEEE, "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements," in *IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003))*, ed, 2005.

[138] "IEEE Draft Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 7: Wireless Access in Vehicular Environments," *IEEE Unapproved Draft Std P802.11p /D7.0, May 2009,* 2009.

[139] M. Boban*, et al.*, "What is the Best Achievable QoS for Unicast Routing in VANETs?," in *GLOBECOM Workshops, 2008 IEEE*, 2008, pp. 1-10.

[140] Y. Gongjun*, et al.*, "Provisioning Vehicular Ad Hoc Networks with Quality of Service," in *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2010 International Conference on*, 2010, pp. 102-107.

[141] N. Zeyun, *et al.*, "Study on QoS Support in 802.11e-based Multi-hop Vehicular Wireless Ad Hoc Networks," in *Networking, Sensing and Control, 2007 IEEE International Conference on*, 2007, pp. 705-710.

[142] "ATR Locations," *State of Georgia,* p. 6, 2010.

[143] J. Benin, *et al.*, "Vehicular network pseudonym distribution in congested urban environments," in *Southeastcon, 2012 Proceedings of IEEE*, 2012.

[144] J. Petit and Z. Mammeri, "Analysis of authentication overhead in vehicular networks," in *Wireless and Mobile Networking Conference (WMNC), 2010 Third Joint IFIP*, 2010, pp. 1-6.

[145] J. Benin, *et al.*, "Impact of pseudonym subsequent pre-computation and forwarding in hybrid vehicular networks," presented at the Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications, Low Wood Bay, Lake District, UK, 2012.

[146] (2011, 3/4/2012). *ISO/IEC 14882:2011: Information technology - Programming languages - C++*. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50372

[147] IEEE, "IEEE Standard Specifications for Public-Key Cryptography," *IEEE Std 1363-2000,* 2000.

[148] Microsoft. (2012, 3/2/2012). *Visual Studio*. Available: http://www.microsoft.com/visualstudio/en-us

[149] GNU. (2012, 3/2/2012). *GCC, the GNU Compiler Collection*. Available: http://gcc.gnu.org/

[150] Z. Jie, "A Survey on Trust Management for VANETs," in *Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on*, 2011, pp. 105-112.

[151] M. Raya, *et al.*, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008, pp. 1238-1246.

[152] U. Minhas, *et al.*, "Towards Expanded Trust Management for Agents in Vehicular Ad-hoc Networks," *International Journal of Computation Intelligence Theory and Practice,* vol. 5, June, 2010.

VITA

JOSEPH T. BENIN

LCDR BENIN was raised in Annandale, Virginia. He attended St. Michael's Roman Catholic School for primary education and Seton High School for secondary. In 2001, he graduated with high honors from the United States Coast Guard Academy with a Bachelor's of Science in Electrical Engineering and a commission in the United States Coast Guard. Upon graduation, he served as a Student Engineer and the Electrical & Electronics Officer aboard the arctic/Antarctic icebreaker USCGC HEALY (WAGB-20), home ported in Seattle, WA. In 2005 he graduated from the Georgia Institute of Technology with Master of Science Degrees in Electrical and Computer Engineering and Information Security with a minor in Public Policy. He returned to the Coast Guard Academy as an instructor and was selected as a member of the Coast Guard's Permanent Commissioned Teaching Staff, whereupon he began his doctoral pursuit. When he is not working on his research, LCDR Benin enjoys reading and engaging in respectful but substantive discussion on religion, politics, and technology. After God, first in his life is his wife, Rachel, followed by his three wonderful children, Rebecca, Joey, and Jeanette.