

PERFORMANCE EVALUATION OF SECURE
COMMUNICATION IN VEHICULAR NETWORKS

by

ASHWIN RAO

Amar Nath and Shashi Khosla School of Information Technology

Submitted

in fulfillment of the requirements of the degree of

Master of Science by Research

to the



Indian Institute of Technology Delhi

January 2009

© Copyright by Indian Institute Of Technology Delhi 2009
All Rights Reserved

CERTIFICATE

This is to certify that the thesis titled “**Performance Evaluation of Secure Communication in Vehicular Networks**” being submitted by **Ashwin Rao** to the Indian Institute of Technology Delhi, for the award of the degree of **Master of Science** by Research in Information Technology, is a record of bona-fide research work carried out by him under our supervision. The work presented in this thesis has not been submitted to any other university or institute for the award of any other degree or diploma.

Dr. Arzad Kherani

Senior Researcher

General Motors India Science Lab.
International Technology Park, Bangalore

Dr. Anirban Mahanti

Assistant Professor

Amar Nath and Shashi Khosla School of IT
Indian Institute of Technology Delhi

Acknowledgment

I would like to thank my advisors, Dr. Arzad Kherani and Dr. Anirban Mahanti, for their guidance and encouragement throughout the course of my study and research at IIT Delhi. Their belief in my abilities motivated me to think harder and their insights guided me throughout my stay here in IIT Delhi. I am deeply indebted to Prof. S. N. Maheshwari for inspiring me to work hard at all times and allowing me to take the course taught by Dr. Arzad Kherani in my first semester without which I would not have come across this project. I would also like to thank Prof. Huzur Saran and Prof. Sanjiva Prasad for permitting my internships, and the researchers at General Motors India Science Lab, Bangalore most notably Dr. Rajeev Shorey, Dr. Bhargav Bellur, Dr. Aditya Karnik, Dr. Aravind Iyer and Anitha Varghese for their assistance and useful feedback. Along with my advisors, I am deeply indebted to Dr. Vinay Ribeiro for introducing me to the various aspects of wireless networks.

Special thanks to all my classmates of the MTech'06 batch and seniors of the MTech'05 batch of the Dept. of Computer Science in IIT Delhi for their constructive criticism of my work and making my time spent here full of fun with tons of memories to cherish. Further, I would like to thank Mrinal Sinha, Rajesh Kumar, S. Negi, and Jaison John who have helped me in many administrative affairs.

My parents are my source of inspiration and this thesis would have been incomplete without their support. It is their endurance that kept me motivated at all times. Finally, I would like to thank all my friends, especially Siddharth Nag, Matin Momin, Alok Mooley, Amit Apte, Aniruddha Patwardhan, Ashvin Agrawal, Manikant Kumar, Vijay Gaji, Sharad Mittal, Sunil Arora, Rajat Mishra and colleagues at Air-Tight Networks especially K. N. Gopinath, Vivek Bhagwat, Dr. Hemant Chaskar, Dr. Deepak Gupta, and Dr. Praveen Bhagwat for encouraging and motivating me to go for graduate studies.

Abstract

This dissertation attempts to evaluate the performance of the Public Key Infrastructure (PKI) based security mechanisms proposed to secure the messages exchanged in vehicular networks, and the performance of communication considering the various overheads of security.

Vehicular networks are not expected to guarantee on-demand connectivity between the principals of the network and the infrastructure responsible for issuing certificates to the principals of network, and revocation of compromised certificates. We propose a metric called *Confidence on Security Infrastructure* to quantify the confidence the principals of vehicular networks can have on the PKI based security given the delays in access to the revocation information due to such sporadic connectivity. We then propose an accept/drop mechanism at the security layer called *Freshness Checks* aimed at controlling these delays. Further, we show that the security performance of vehicular networks is independent of the density of the vehicles if one only takes vehicle reliability into account however, intentional malicious activities could require an increase in infrastructure presence.

The proposed safety applications rely heavily on secure exchange of data using the broadcast services of the MAC layer. Further, any security mechanism comes with overheads in terms of computation and communication. We show that the computational overheads of the proposed PKI based security result in packet processing and not packet transmission becoming a bottle-neck. Further, broadcast packets that undergo collisions are not retransmitted. We obtain this collision probability by initially assuming low rates of packet generation at the application layer resulting in our nodes being bufferless at the MAC layer and then extend our model for finite buffers to study the system under higher data traffic loads. We show that adapting packet generation rates and the time for which a message is transmitted over the air have a greater impact on packet losses due to collisions as compared to adapting the probability of attempting a transmission and buffer sizes at the MAC layer.

Contents

Acknowledgment	iii
Abstract	v
1 Introduction	1
1.1 Motivation	2
1.2 Objectives	3
1.3 Contribution	4
1.4 Organization	5
2 Background and Related Work	7
2.1 Applications Envisioned For Vehicular Networks	7
2.1.1 Parameters to Characterize Safety Applications	8
2.1.2 Cooperative Collision Warning (CCW)	9
2.2 Security In Vehicular Networks	10
2.2.1 Need For Securing Vehicular Networks	10
2.2.2 Cryptographic Techniques	11
2.2.3 Security Using Public Key Infrastructure	13
2.3 IEEE 1609 Protocol Stack	17
2.3.1 IEEE 802.11	18
2.3.2 IEEE 1609.4	20
2.3.3 IEEE 1609.3	22
2.3.4 IEEE 1609.2	23
2.3.5 IEEE 1609.1	24
2.4 Related Work	25
2.4.1 Securing Vehicular Networks	25
2.4.2 Modeling Vehicular Communication	27
2.4.3 Modeling IEEE 802.11	28
2.5 Summary	29
3 Performance of Security in Vehicular Networks	31
3.1 Dilemma at Receivers	31
3.2 Confidence on Security Infrastructure	33
3.3 Freshness Check Scheme	34

3.3.1	Freshness of Certificates	36
3.3.2	Advantages and Disadvantages of Freshness Checks	38
3.4	Modeling Security Performance	39
3.4.1	Performance of CRL Based Schemes	42
3.4.2	Performance of Freshness Check Scheme	46
3.5	Numerical Results	50
3.5.1	Performance of CRL based schemes	51
3.5.2	Performance of Freshness Check Scheme	54
3.6	Summary	62
4	Performance of Communication in Vehicular Networks	63
4.1	Overheads of Security	63
4.2	Impact of Computational Overheads	65
4.2.1	Queuing at Security Layer	66
4.2.2	Simulation Framework to Study Queuing System	68
4.2.3	Numerical Results and Discussions	69
4.3	Performance of Broadcast Communication	73
4.3.1	System Model: Assumptions and Notations	73
4.3.2	Modeling Bufferless MAC	74
4.3.3	Modeling MAC with Finite Buffers	77
4.3.4	Numerical Results and Discussions	83
4.4	Summary	89
5	Conclusions and Future Work	91
5.1	Summary and Conclusion	91
5.2	Future work	92
	References	94
A	Simulating Security Overheads	101
A.1	Design for Security Layer in ns2	101
A.2	Algorithm For Abstracting MAC Layer	103

List of Figures

2.1	Symmetric Key Cryptography	12
2.2	Asymmetric Key Cryptography	14
2.3	Components Of The IEEE 1609 Protocol Stack	18
2.4	Priority Queues in IEEE 1609.4	20
2.5	Inter-frame sequences in IEEE 1609.4	21
2.6	Structure of a Signed Message in IEEE 1609.2	23
2.7	IEEE 1609.1 Modules	25
2.8	Markov Chain Model for Backoff Window Size	28
3.1	Dilemma at receivers in CRL based scheme	33
3.2	Accept/Drop mechanism in Freshness Check scheme	35
3.3	Operations during Freshness check	37
3.4	Categorization of packets in CRL based schemes	43
3.5	Possible instants of revocation in Freshness Check Scheme.	47
3.6	False Negatives as Idle Periods of G/D/ ∞ queue.	48
3.7	Topology used in simulations.	50
3.8	Inter-meeting times.	51
3.9	CoS when revocation occurs due to faults in devices.	52
3.10	CoS when revocation is due to intentional misbehavior.	53
3.11	Evolution of the time for which a $M/D/\infty$ queue is idle.	54
3.12	Impact of node density and Freshness Check Threshold	55
3.13	Impact of Freshness Check Threshold	56
3.14	Impact of revocation rate	57
3.15	Comparison of CRL and Freshness Check scheme	58
3.16	Impact of node density	60
3.17	False Positives when revocation occur due to intentional misbehavior	60
3.18	False Negatives when revocation occur due to intentional misbehavior	61
3.19	True Positives when revocation occur due to intentional misbehavior .	61
4.1	Overheads of Security	64
4.2	Queueing at the Security Layer	65
4.3	Queueing at the Security Layer and the MAC Layer	68
4.4	Packets lost to collisions when there are no delays at security layer. .	70
4.5	Time spent at the security queue of the source of the packet.	71
4.6	Number of nodes successful in sending packets to the MAC layer. . .	71

4.7	Packets lost to collisions when there are delays at security layer . . .	71
4.8	Broadcast of fixed size packets	75
4.9	Two State Markov chain for a node	75
4.10	Markov Chain for a node with finite buffer	77
4.11	Impact of packet generations rates on performance of Bufferless MACs.	84
4.12	Impact of busy period lengths on performance of Bufferless MACs. . .	84
4.13	Impact of probability of transmission attempts in Bufferless MACs. .	85
4.14	Probability of finding a node in State i ($0 \leq i \leq K$) when $K = 3$. . .	86
4.15	Impact of packet generations rates in systems with finite buffers. . . .	87
4.16	Impact of probability of transmission attempts in finite buffer systems.	87
4.17	Impact of length of busy periods in systems with finite buffers.	87
4.18	Impact of buffer size in systems with finite buffers.	88
A.1	Timing values stored in individual packets	102
A.2	Trace File Format	103

Chapter 1

Introduction

The ever increasing number of road vehicles and their associated traffic hazards has resulted in a large number of safety devices like laser scanners, ultrasonic, and vision based sensors being built into road vehicles. These devices assist the drivers, however one major limitation of such devices is their short range of operation. The evolution of wireless communication as a dependable source of information exchange has motivated governments and automobile manufacturers to promote wireless technologies to extend the drivers horizon by allowing vehicles to communicate with each other. Vehicle Safety Communication (VSC) [1], Car to Car Consortium (C2C) [2], Network On Wheels (NOW) [4], Partners for Advanced Transit and Highways (PATH) [5], and Secure Vehicle Communication (SeVeCom) [6] are some of the consortia promoting research in the area of vehicular communication. The rapid research in the area of *vehicular ad hoc networks* has conceived a number of applications to enhance the safety of passengers and the efficiency of the transportation system.

A mobile ad hoc network (MANET) is an ad hoc network, i.e., a self-configured network generated on the fly, of mobile nodes connected by wireless links. These nodes are free to move randomly and organize themselves indiscriminately. A vehicular ad hoc network (VANET) is a special kind of MANET in which the mobile nodes are vehicles. The main difference between VANETs and MANETs is that the nodes in VANETs move in a random and relatively predictable manner at much higher speeds compared to traditional MANETs, causing sporadic creation and breaking of wireless links. The advantage of VANETs over traditional ad hoc networks is that the nodes (vehicles) possess substantial power resources. Like all communication networks, VANETs are vulnerable to attacks from malicious and malfunctioning nodes, motivating the need for securing vehicular networks. This dissertation attempts to evaluate the performance of the security mechanisms proposed to secure the messages

exchanged in vehicular networks, and the performance of communication considering the various overheads of security.

1.1 Motivation

VANETs allow vehicles to communicate with other vehicles (vehicle-to-vehicle or V2V) and the roadside infrastructure (vehicle-to-infrastructure or V2I) in its vicinity for applications that increase drivers awareness of the surroundings thus enhancing safety and possibly optimizing traffic. Bai *et al.* [18], group the applications envisioned for vehicular networks into 3 classes: safety-oriented, convenience-oriented and commercial-oriented. The safety-oriented applications (safety applications) aim to assist drivers in handling upcoming events and potential danger. Like all communication networks VANETs are vulnerable to attacks by misbehaving entities. Messages exchanged for safety can be spoofed, modified, or falsely generated by such nodes. Hence, a primary requirement of the safety applications is quick and reliable exchange of safety related data, motivating the need for securing the messages exchanged.

The IEEE 1609.2 standard [9], a part of the proposed IEEE 1609 protocol stack for Wireless Access in Vehicular Environments (WAVE), defines the secure message formats and techniques required for processing the secure messages. The technique proposed for authentication and ensuring integrity of the messages is based on the Public Key Infrastructure (PKI). In PKI, a centralized entity known as the Certifying Authority (CA) is responsible for certifying the status (misbehaving or trustworthy) of the individual nodes and is responsible for eviction of malicious and other misbehaving nodes. Packets generated from such misbehaving nodes need to be rejected which is possible only if the latest information regarding the trustworthiness of the message source is available by all recipients. Wired networks can guarantee *on demand connectivity* between the CA and principals in the wired network for obtaining the current status of any source that uses PKI to secure its messages. Such on demand connectivity with the centralized entity is essential for recipients to have *confidence on the security infrastructure*. Vehicular networks cannot guarantee such on demand

contact at all times due to the sporadic connectivity caused by the mobility of vehicles and the costs involved in using other communication technologies like cellular and satellite links, hence, the confidence on the security infrastructure in vehicular networks *needs to be quantified*.

The security of messages come with their own processing and bandwidth overheads that can affect the performance and scalability of vehicular networks. Traditional performance modeling of wireless networks consider packet transmissions to be the main bottleneck, hence, they revolve around modeling the lower layers of the protocol stack. The extensive number of applications relying on the broadcast services of the lower layers, and the computationally heavy security services of the security layer motivate the need for modeling the packet processing along with packet transmission for studying secure vehicular communication. The lower layers of the wireless protocol stack has been studied in great detail however these studies have been restricted to unicast traffic to a *large extent*. Safety applications for vehicular networks rely heavily on broadcast communication where retransmissions are not employed due to the stringent latency requirements of the messages and the desire for recent information. The absence of retransmissions motivate the need to remodel the lower layers for broadcast communication.

1.2 Objectives

The objectives of this thesis are as follows.

1. **Performance modeling of security in vehicular networks:** This involves analyzing the impacts of sporadic connectivity with the security infrastructure on the security performance of the proposed security mechanisms.
2. **Performance modeling of communication considering the impacts of security:** This involves modeling vehicular communication considering the impact of the various overheads of security and modeling the lower layers for broadcast traffic.

1.3 Contribution

Performance evaluation of secure communication in vehicular networks involves the performance of the security proposed for communication in vehicular environments and the performance of the communication considering the various impacts of security. The sporadic connectivity between the principals of vehicular networks and the infrastructure puts the recipients of secure messages in a dilemma regarding the legitimacy of the source of the message. We coin a metric called Confidence on Security Infrastructure (CoS) that quantifies the confidence the principals of vehicular networks can have on the security provided by the security infrastructure given such sporadic connectivity. We show that this metric can be used to obtain the required infrastructure presence. Further, if misbehavior is only due to faults developed in the devices involved in the vehicle-to-vehicle (V2V) system, we show that the infrastructure requirement for a desired CoS is independent of the penetration of V2V enabled vehicles. We also propose a technique called *Freshness Check* that enables the source of secure messages to provide the recipients of the messages the last time the infrastructure considered the source to be a legitimate node. We show that when revocation occurs only due to faults developed, the Freshness Check scheme can provide a better security performance compared to the CRL based schemes in regions of low infrastructure presence or when the costs of communicating the infrastructure are high.

Traditional models of communication performance do not consider the computational overheads of packet processing at the source and destination. In this thesis we study the impacts of the computational and bandwidth overheads of security on the communication performance of vehicular networks. We find that computations required for security and not packet transmissions are the bottlenecks for the security mechanisms currently proposed in the IEEE 1609.2 standard. These proposed safety applications exchange messages using the broadcast services of the lower layers of the protocol stack. The broadcast packets undergoing collision are not retransmitted, hence, obtaining the collision probability thus becomes critical for the success of applications relying on broadcast communication. We show that adapting packet

arrival rates and packet lengths have a greater impact on packet collision probability compared to adapting the probability of attempting a packet transmission and buffer sizes at the MAC layer.

1.4 Organization

The remainder of this thesis is organized as follows. Chapter 2 provides an overview of the proposed applications and the techniques proposed for securing the messages exchanged by these applications. It also provides an overview of the proposed protocol stack for vehicular networks and discusses the related work in modeling the communication performance and security performance of vehicular networks. We propose a metric called Confidence on Security Infrastructure (CoS) and propose a technique called Freshness Checks for accepting/rejecting messages at the security layer in Chapter 3. The impacts of security on the communication performance of vehicular networks is discussed in Chapter 4. The conclusions and the directions for future work are presented in Chapter 5.

Chapter 2

Background and Related Work

This chapter provides a brief overview of the current scenario in the area of security in vehicular networks. Section 2.1 gives some important parameters required to classify the proposed applications with the Cooperative Collision Warning (CCW) application as an example. These applications are vulnerable to attacks by attackers that might interfere with the system for fun and or profit. Section 2.2 enumerates the security mechanism commonly used in the area of computer networks. Section 2.3 provides a brief overview of the various components of the protocol stack proposed for secure vehicular communication. The literature survey in the area of securing vehicular networks and modeling the key components of the protocol stack is given in Section 2.4

2.1 Applications Envisioned For Vehicular Networks

The research community has proposed a number of potential applications based on vehicular networks ranging from safety/warning to infotainment, a few of which are mentioned in Table 2.1 [15; 18; 38]. Bai *et al.* [18], classify the applications as follows:

1. **Safety applications:** These applications attempt to increase the drivers awareness of the surrounding thus assist the drivers in handling events critical to the safety of passengers.
2. **Convenience applications:** These applications are centered around enhancing the traffic efficiency and improving the convenience of passengers.
3. **Commercial applications:** These applications provide the passengers of the vehicle with various types of services including those that can enhance the travel experience.

Application Name	Description	Category
Emergency Electronic Brake Light (EEBL)	A vehicle braking hard broadcasts a warning message	Safety
Cooperative Collision Warning (CCW)	A vehicle monitors the status of vehicles in the neighborhood to warn of potential collisions	Safety
Post Crash Notification (PCN)	A vehicle involved in an accident broadcasts of the accident until the site is cleared	Safety
Emergency Vehicle Alert	On coming emergency vehicles warn others of their existence	Safety
Parking Availability Notification	A vehicle queries for parking lots in a region	Non-safety (Convenience)
Toll Payment	Vehicle pay tolls	Non-safety (Commercial)
Service Announcements	Businesses announce their services in a region	Non-safety (Commercial)

Table 2.1: Proposed Safety and Non-Safety Applications

The proposed applications vary on their requirements especially in their allowable end to end latencies. Kroh *et al.* [38], provide details of the application requirements such as time constraints and the desired contents of messages exchanged. Some of the end to end delays are as follows:

1. Up to 0.5 seconds for highly critical messages like Intersection Collision Warning.
2. Up to 1 second for time critical messages.
3. Up to 5 seconds when the time is relevant; for example, notification for glare reduction.
4. Around 10 seconds when time is not critical; for example, Intelligent Traffic Flow-control.

2.1.1 Parameters to Characterize Safety Applications

Safety application are the main motivation for vehicular networks, hence, these applications are widely used in studying the performance of vehicular networks. Further, the parameters used to characterize these applications are essential for modeling these applications and abstracting them for simulations. A comprehensive set of these parameters available in [15; 18], some of which are as follows:

1. **Type of Communication:** It considers point-to-point, point-to-multi-point, vehicle-to-vehicle, vehicle-to-infrastructure, infrastructure-to-vehicle etc.
2. **Transmission Mode:** It describes whether the transmission is triggered by an event or sent automatically at regular intervals.
3. **Minimum Frequency:** It defines the minimum rate at which a transmission should be repeated.
4. **Allowable Latency:** It defines the maximum duration of time allowable between when information is generated for transmission and when it is received.
5. **Data to Be Transmitted and/or Received:** It describes the contents of the communication.
6. **Maximum Required Range of Communication:** It defines the maximum communication distance between two entities that is required to effectively support a particular application (e.g., 150 m to avoid multi-hop).
7. **Event lifetime:** It specifies how long an application event persists in time. The applications can be classified as short lifetime events like EEBL that last a few seconds or long lifetime events like PCN that can last for a few hours.

2.1.2 Cooperative Collision Warning (CCW)

Parameter	Description
Communication Type	Point to multi-point
Transmission Mode	Periodic
Minimum Frequency	10 Hz
Allowable Latency	100 ms
Data Transmitted and Received	Position, Velocity, Acceleration and Direction
Minimum Communication Range	150 meters

Table 2.2: Parameters For Messages Exchanged By CCW Applications

One of the proposed safety applications is Cooperative Collision Warning (CCW). CCW actually represents a class of applications where each vehicle (capable of vehicular communication) monitors the kinematics status messages from vehicles in its

neighborhood to warn of potential collisions [15]. Some of the parameters for the messages exchanged by the CCW class of applications are given in Table 2.2 [15; 18].

One reason for generating messages at 10 Hz (once every 100 milliseconds) is given by Xu *et al.* [68]. At 150 *km/hour* (approximately 40 meters/sec) a vehicle travels about 4 meters in 100 milliseconds. Updates arriving at rates higher than 10*Hz* would provide of information of travel less than a car length while updates arriving at lower rates *might* results in drivers detecting the potential hazard before the system. The communication range of 150 meters is proposed to circumvent the need for multi-hop [15]. Though the speeds mentioned are on the higher side, they give a good insight on the bounds for the parameters under consideration.

The low latency and high packet generation rates of CCW result in a considerable network and processing load, hence, this application has received a lot of attention and is widely used for modeling vehicular networks in [15; 18; 27; 28; 38; 62; 69].

2.2 Security In Vehicular Networks

Vehicular networks like all communication networks are vulnerable to attacks by misbehaving entities that can affect the performance of the system. Section 2.2.1 motivates the need for security by enumerating some of the attacks possible with their impacts. Section 2.2.2 provides the cryptographic techniques currently used to secure traditional communication networks.

2.2.1 Need For Securing Vehicular Networks

Misbehavior can be due to intentional malicious activities or due to faults developed in devices required for generating and transmitting data in vehicular networks. A set of potential attacks and their classifications are available in [16; 47; 53]. Some of these attacks are as follows:

1. **Fabrication Attacks:** These include attacks where the adversary broadcasts fabricated data. For example, the adversary could inject false location information in CCW messages to generate warnings for potential collisions.

2. **Message Suppression Attacks:** It includes the attacks where the attacker selectively drop packets from the network. For example, alerts for road condition hazards like oil spills could be dropped.
3. **Alteration Attacks:** These attacks include the retransmitting of modified information, delay in transmission of information etc. For example, the adversary could modify the contents of EEBL messages to indicate a different location of hard braking.

A considerable research attention has been received for defining the primitives of the system providing security in VANETs. The list of such primitives required for applications like CCW where the content of the message need not be encrypted are as follows [26; 47; 48; 53].

1. **Authentication:** There can be malicious and genuine sources for the messages exchanged. Authentication is the ability to distinguish between these sources.
2. **Anonymity:** The physical identity of the originator of a message should not be easy to extract from the message. Though the extent of anonymity is debatable, its existence is essential for privacy of the users of vehicular communication.
3. **Non repudiation:** The sender of a message should not be able to deny having sent the message.
4. **Data Integrity:** The data received is exactly as sent by the source of the message.
5. **Low Overhead:** The messages being time critical, the security overheads should retain the usefulness of the message.

The services of the security system providing the desired security are based on the cryptographic techniques mentioned below.

2.2.2 Cryptographic Techniques

Cryptography is the study of the design of techniques for ensuring the secrecy and/or authentication of information [61]. The three main types of cryptographic techniques are symmetric key algorithms, asymmetric key algorithms and hash functions.

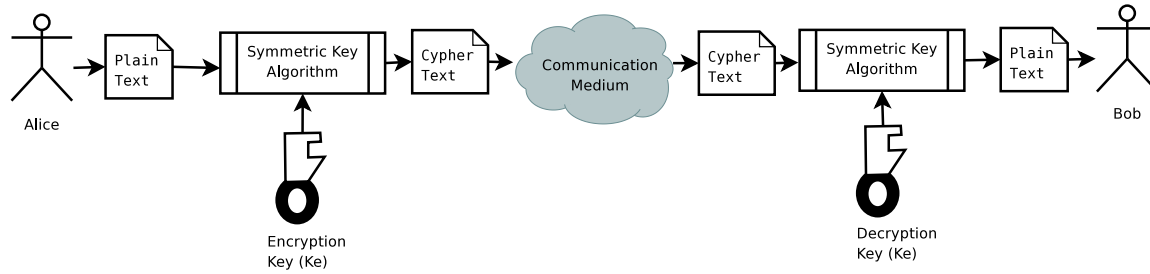


Figure 2.1: Symmetric Key Cryptography

2.2.2.1 Symmetric Key Algorithms:

In symmetric key cryptography, the entities that communicate securely have access to a secret data known as a *key*. This key is used to encrypt the data at the source and the same key is used to decrypt the data at the receiver of the message. The exchange of messages takes place using 2 functions $E(\cdot, \cdot)$ and $D(\cdot, \cdot)$ to encrypt and decrypt the message, having the property $E_M = E(K, M)$ and $M = D(K, E_M)$, where K is the key used to secure the message M . E_M is the message that is transmitted by the source and received by the intended and unintended recipients of the message. A major problem that needs to be addressed in systems secured using symmetric keys is the exchange of keys between the communicating entities.

2.2.2.2 Asymmetric Key Algorithms:

In asymmetric key cryptography, each principal that is a source of a message has a pair of keys: Private Key, Public Key. The *private key* is known only to the principal, whereas the *public key* can be shared with all the entities in the system without jeopardizing the security of the private key. The keys can be visualized as a pair of functions $P_r(\cdot)$ and $P_u(\cdot)$ representing the private and public keys respectively, having the property $M = P_r(P_u(M))$ and $M = P_u(P_r(M))$, where M is the message that is to be secured using the keys. A major problem in this system is to know the genuine mapping between the public key, the private key and the owner of the private key.

Hash Function	Input String	Hash Value
MD-5	Need for hashing	cdd5e180750ee8ac7703627f5ba5d3db
MD-5	Need for hashin	af7f67efb56cfecb043c79a6b96392c2
SHA-1	Need for hashing	b841de2d50f19767b0d1ccf3ff007befbcfaf9ce
SHA-1	Need for hashin	2946b3a413e88f983c23266e2f9cb10c6eff8837
SHA-224	Need for hashing	b3757c331b30459254c5069fc12f52282b2ee1a605b1f9ed635a3657
SHA-224	Need for hashin	c02a3d411743ff29704cd5387a6909746d7dbc2dfde97acaba164c22

Table 2.3: Hash Values From Different Hash Functions

2.2.2.3 Hashing Functions:

The hash function (h) maps an *arbitrary* length input to a fixed length output ($h(x)$). They are typically used for data integrity, where the hash of the message is sent with message, and/or for authentication, where the hash is computed using the message and a key as input. For securing the messages, the hash functions in cryptography have the following properties [43].

1. **Pre-image Resistance:** It should be computationally infeasible to compute a pre-image x' for any given y such that $h(x') = y$.
2. **2nd Pre-image Resistance:** Given any x and $h(x)$, it should be computationally infeasible to find an x' such that $x' \neq x$ and $h(x') = h(x)$.
3. **Collision Resistance:** It should be computationally infeasible to find any x and x' such that $h(x) = h(x')$.

The output of the hash function is typically known as hash value or message digest. Table 2.3 shows the output of the MD-5, SHA-1 and SHA-224 hash functions when the strings “Need for hashing” and “Need for hashin” are provided as input, highlighting that a small change in input results in a considerable change in the hash value.

2.2.3 Security Using Public Key Infrastructure

One of the major shortcomings of symmetric key crypto-systems is the need for a secure key distribution channel. Further, n entities result in $\frac{n(n-1)}{2}$ potential pairs who may wish to communicate privately with each other resulting in a large number of secret keys exchanged and maintained.

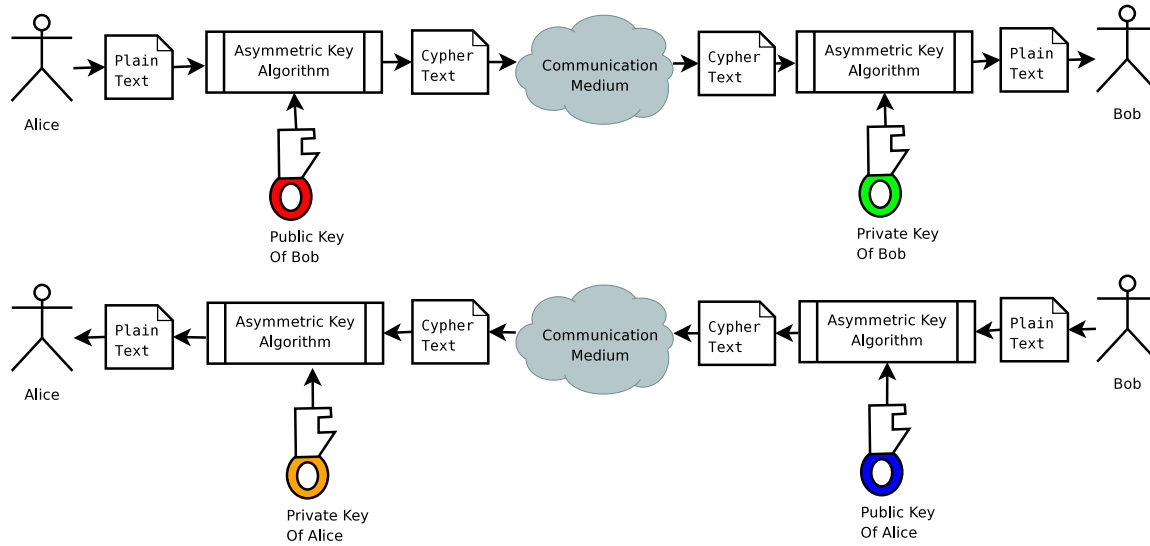


Figure 2.2: Asymmetric Key Cryptography

Diffie *et al.* [24], in the seminal work motivating digital signatures propose a public key crypto-system based on asymmetric key cryptography for providing authentication, non-repudiation and privacy. The RSA algorithm for such public key crypto-systems was proposed by Rivest *et al.* [55]. In a asymmetric key based crypto-systems if Alice wants to send a message to Bob, she uses the public key of Bob which ensures that only Bob can decrypt the message. Similarly, if Bob wants to broadcast a message, he uses his private key to secure the message. A road-block in this approach is, “How can Alice be sure that the private key used is Bob’s private key?”.

Public Key Infrastructure (PKI) helps solve the problem of exchange of keys without compromising them by using trusted nodes known as Certificate Authorities (CA) to digitally sign data structures known as *certificates*. These certificates attest the binding between the owner of the private keys to its corresponding public keys. An (unsigned) certificate has several fields including:

1. The certificate serial number that is unique for a certificate
2. The public key.
3. The expiry time of the certificate.

The certificate issued by the CA also contains the signature of the CA. Note that the *Public Key of the CA* must be available at each entity of the PKI system in order to verify the certificates signed by the CA. Such digital certificates are the building blocks of the (PKI). To ensure message integrity and authenticity, the source of the message *signs* the (hash of the) message with its private key, and appends this *signature* along with the message. Upon receiving this message, the recipient can verify the signature of the message using the public key, the dual of the senders private key. This technique has been proposed for safety applications in vehicular networks where authentication of the message source and data integrity are vital.

Communication networks are vulnerable to malicious or malfunctioning nodes whose eviction is possible only when the CA revokes the certificates issued to them. Only the nodes in possession of this revocation information can *confidently* reject the packets sent by the revoked nodes. Detection of such misbehaving nodes and propagation of revocation information is thus vital for the success of networks relying on PKI for security. Some of the techniques used for propagation of the revocation information are as follows:

1. In the *push* model, the CA sends the revocation information at regular intervals.
2. In the *pull* model, the verifiers download the revocation information from the CA as and when needed.
3. In the hybrid approach the revocation information is periodically *pushed* to several intermediate repositories (called Directories) from which the verifiers may *pull* the revocation information.

Kocher *et al.* [37], provide the important requirements for any revocation system, these include:

1. **Reliability:** The revocation service must be available at all times.
2. **Memory:** Minimum amount of memory should be required as validation is often carried out in constrained environments¹.

¹In the case of vehicular networks, validation shall be carried by the on board devices that shall have limited memory compared to traditional workstations and servers

3. **Bandwidth:** Communication bandwidth should be minimal.

Certificate Revocation Lists (CRLs) is the simplest technique for propagation of revocation information. A CRL is a list containing the certificate serial numbers of all the certificates that were revoked at the time when the CRL was released. This list is digitally signed to avoid spurious CRLs. One of the important short-comings of the CRL based approach for vehicular networks is the limited storage capacity of vehicles compared to traditional workstations. Another important problem to be addressed is the propagation of the CRLs to all the *concerned* vehicles irrespective of their current geographic location and mobility. One of the first solutions to address the issue of scalability of CRLs was *delta-CRLs*. When CRLs are infrequently issued by the CA, delta-CRLs are issued that contain the revocation between two CRL issues. Adams *et al.* [14] extend delta-CRLs by a concept called *Freshest delta-CRL* that contains the latest revocation information. *Windowed Certificate Revocation* [42] and *Sliding Window Delta-CRLs* [23] are other variants of addressing the problems of traditional CRLs mentioned by Kocher *et al.* [37], and Slaggel *et al.* [59].

A counter-part to propagation of revocation information is on demand checking of the certificate status. On-line Certificate Status Protocol (OCSP) [44] proposes an on demand validation of certificates. The verifier issues an OCSP request, that contains the list of certificates to be validated, to a trusted server representing the CA. The server responds by with the time stamp of the request and the status of the individual certificates present in the *OCSP request*. This response is signed either by the server or by the CA. The Simple Certificate Verification Protocol (SCVP) [29] provides a certificate validation protocol that is capable of handling the complete certificate validation process. These techniques though practical in wired networks are impractical in vehicular networks due to the stringent latency requirements of the applications.

Despite the short-comings related to propagation of revocation information, the need for trusted authorities like CAs to ensure authentication has motivated researchers to propose PKI based security for vehicular networks [33; 36; 46; 45; 71]. One such proposal by Papadimitratos *et al.* [46] consists of the following entities:

1. **Authorities:** The authorities are trusted entities such as organizations responsible for registration of vehicles. They are responsible for the management and the credentials of the principals in vehicular networks.
2. **Trusted Components:** The trusted components include the built-in hardware and firmware that perform cryptographic operation, such as signing and verifying of messages, and storage of the data involved in the security operations.
3. **Vehicle Identification and Credentials:** Each vehicle represents the on-board central processing and communication module. It has at least a pair of private and public keys. The binding of the vehicle to the keys is done by the authorities by issuing a digital certificate.

The rapid research in the area of vehicular communication has motivated the need to standardize a protocol stack for vehicular networks. The IEEE 1609 family of standards provides a communication protocol stack for secure vehicular communication. The next section provides a brief overview of the various components of the proposed protocol stack and the IEEE 802.11 standard from which the medium access and control (MAC) layer for this stack is inspired.

2.3 IEEE 1609 Protocol Stack

Dedicated Short Range Communication (DSRC), the wireless technology proposed to vehicular communication, provides wireless communication over line-of-sight distances of less than 1000 meters [7]. The IEEE 1609 family of standards provide a communication protocol stack for vehicular networks, also known as Wireless Access in Vehicular Environments (WAVE), based on DSRC.

The 2 types of WAVE devices supported by IEEE 1609 are:

1. Road Side Unit (RSU) - RSUs are DSRC transceivers that operate only when stationary. They support information exchange with On Board Units (OBUs) and can be visualized as access points of IEEE 802.11 networks.
2. On Board Unit (OBU) - OBUs are DSRC transceivers present in vehicles that can operate when vehicles are in motion. They support information exchange

Resource Manager IEEE 1609.1	Describes the key components of the WAVE system architecture
Security Services IEEE 1609.2	Defines the secure message formats and the processing required for each of these messages
Networking Services IEEE 1609.3	Equivalent to the network and transport layer of the OSI model
Multi-Channel Operations IEEE 1609.4	Equivalent to the data link layer of the OSI model.

Figure 2.3: Components Of The IEEE 1609 Protocol Stack

with RSUs and other OBUs. An important subset of OBUs is the Public Safety On Board Unit (PSOBU), that are embedded in public safety vehicles, like ambulances, and operate public safety applications.

At the physical layer WAVE distinguishes between two classes of radio channels. The spectrum is proposed to be divided into seven channels: one control channel (CCH) and six service channels (SCH) [15]. The transmit power in these channels are proposed to be in the range of 23 dBm to 33 dBm, the details of which are available in [7].

The medium access layer for vehicular communication, IEEE 1609.4, is based on the IEEE 802.11 standard [10]. We now see some of the details of the IEEE 802.11 standard.

2.3.1 IEEE 802.11

In wireless networks, the source of a packet, unlike their wired counter-parts in most wired networks, cannot *detect* collisions (easily) at the intended receivers motivating the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) technique that attempts to avoid collisions. A wireless station with a packet to transmit initially monitors the channel activity for the Distributed Inter-Frame Space (DIFS) time period. If the channel is (or becomes) busy during this observation period, the station begins the *back-off* process. The station then chooses a back-off counter in the range $(0, w)$, where w is the contention window. This back-off time represents a counter that is decremented each time the channel is sensed idle, frozen when transmission is

detected in the channel, and decremented when the channel is sensed idle again for more than one DIFS. The station transmits when this counter reaches zero.

The IEEE 802.11 CSMA/CA does not perform collision detection by listening on the channel while its transmission is in progress. Thus, *unicast* transmissions result in transmission of a positive acknowledgment from the receiver, the absence of which is considered to be a failure of successful reception of the packet at the receiver. The DCF adopts an exponential back-off mechanism for unicast transmissions in the event of such losses. The initial value of w is set to CW_{min} , the minimum contention window, and is doubled after each unsuccessful transmission up to a maximum value $CW_{max} = 2^m CW_{min}$, where m is the maximum back-off stage. This process of retransmission continues until a threshold number of retransmission attempts are made or until a positive acknowledgment is received.

As the source cannot detect the channel activity at recipients wireless networks suffer from the hidden terminal problem which is explained as follows. Consider 3 nodes A, B and C such that A and B are in communication range of each other. Similarly B and C are in communication range of each other while A and C are not. While A is transmitting to B, C cannot detect the transmissions at B, hence can falsely detect the channel to be idle (at B) and start transmission resulting in collisions at B. This problem is addressed for unicast communication in IEEE 802.11 based wireless networks by the RTS/CTS mechanism [13]. The RTS/CTS scheme assumes that the transmitter A shall send a (Request to Send) RTS to B which shall respond by a (Clear to Send) CTS to A. Nodes that can listen to the RTS and CTS, i.e., nodes in the communication range of A and B, can now *virtually sense* the medium around A and B to be busy. The acknowledgment of received data from B specifies that the channel is now idle and available for contention. This mechanism though suitable for unicast traffic is not practical for broadcast traffic where the intended audience of the packet, i.e., receivers of RTS and transmitters of CTS, is not known. Similarly waiting for acknowledgment from each of the receivers to determine the channel to be idle is also impractical. Broadcast packets are hence not acknowledged by the recipients in vehicular networks. Thus, the source has no idea whether the packet is successfully

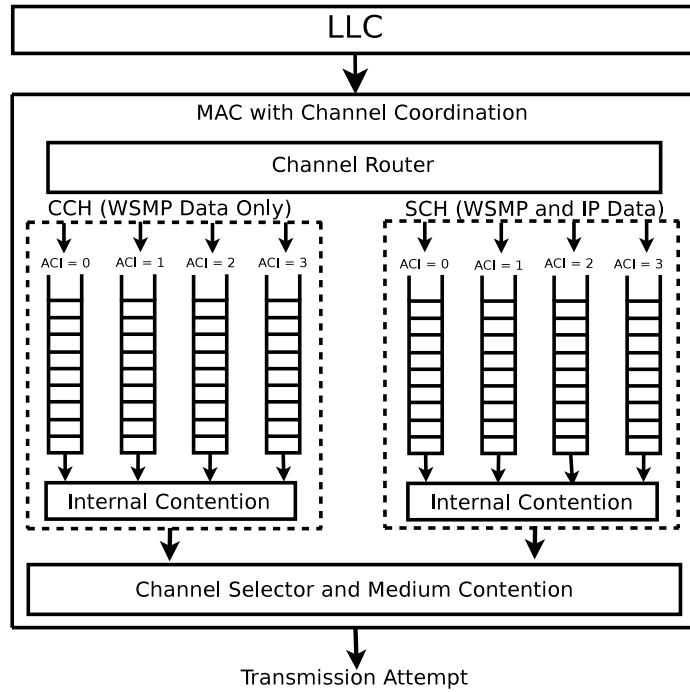


Figure 2.4: Priority Queues in IEEE 1609.4

received by the intended recipients (if any) or not resulting in no retransmission of packets that are lost in the wireless medium. Thus applications for vehicular networks like CCW rely on period broadcast of packets hence cannot be modeled like a network using unicast traffic.

2.3.2 IEEE 1609.4

WAVE devices are proposed to use to the control channel (CCH) for short and high priority messages like safety messages. Service channel (SCH) visits are arranged via a Wave Basic Service Set (WBSS), formed to exchange other non-critical data.

The IEEE 1609.4 standard provides modifications, notably prioritized access to the physical channel similar to the IEEE 802.11 standard [8; 13], to support WAVE operations. The general frame formats of the MAC layer service data units and the management frames are similar to those used in IEEE 802.11. Some important definitions given in [10] are:

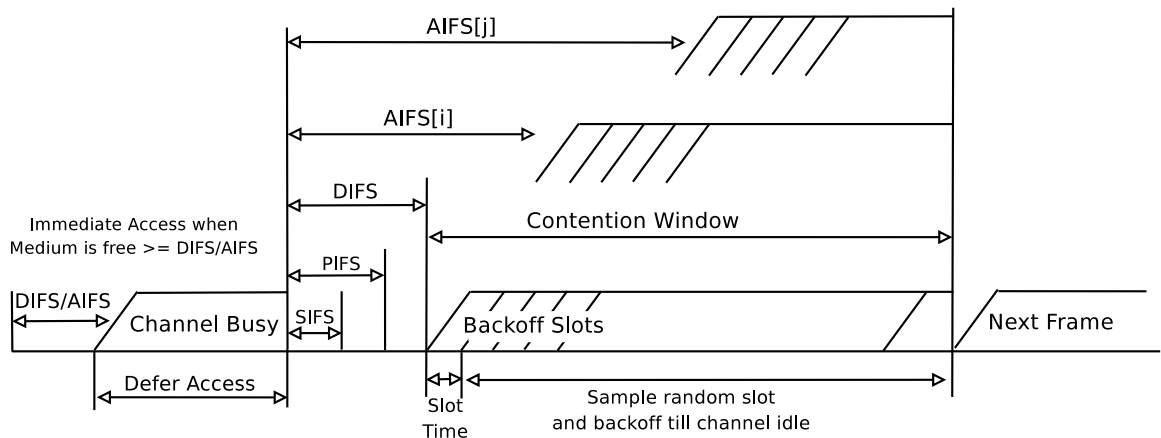


Figure 2.5: Inter-frame sequences in IEEE 1609.4

1. **Enhanced Distributed Channel Access (EDCA):** A prioritized CSMA/CA mechanism for quality of service (QoS).
2. **Access Category (AC):** A label for EDCA parameters that used by stations for channel contention.

The various inter-frame spaces in [10] to ensure prioritized channel access are as follows:

1. *SIFS* - Short Inter-frame space is used for the highest priority transmissions.
2. *PIFS* - Point Coordinated Function (PCF) Inter-frame Space: It is used by the centralized controller (point coordinator) in PCF scheme when issuing polls.
3. *DIFS* - Distributed Coordinated Function (DCF) Inter-frame Space: When the radio link has been free of any traffic for a period greater than the DIFS, stations may have immediate access to the medium in a contention based service. It is used as minimum delay for asynchronous frames contending for access
4. *AIFS* - Arbitration Inter-frame Space: The AIFS is used by QoS stations to transmit data frames, management frames, and some of the control frames.

The important parameters used during channel contention are:

1. *Arbitration inter-frame space (AIFS):* It is the minimum time interval between the wireless medium becoming idle and the start of transmission of a frame.

2. *Contention window (CW)*: It is an interval from which a random number is drawn to implement the random back-off mechanism.
3. *Transmit opportunity (TXOP) limit*: It is the maximum time duration (in milliseconds) for which a station can transmit after obtaining a TXOP.

The internal contention (*virtual contention*) is resolved by computation of the back-offs independently for each AC followed by selection of the AC with the smallest back-off value that contends externally for the wireless medium.

Like traditional networks the services of this layer shall be used by the network and transport layer which has been standardized for the WAVE protocol stack as the IEEE 1609.3 standard, an overview of which is given below.

2.3.3 IEEE 1609.3

The IEEE 1609.3 standard [12] defines network and transport layer services in support of *secure WAVE data exchange*. It defines the Wave Short Messages (WSM), that is an alternative to IPv6 for application using the WAVE protocol stack. It consists of two planes, the management plane and the data plane.

In the data plane, the data can be transmitted using the Wave Short Message (WSM) Protocol (WSMP) or using IPv6. The WSMP is unique to the IEEE 1609 as it provides control to the transmission power, channel and data rate on a frame by frame basis. Safety applications like CCW have been proposed to use the WSMP.

A number of services are associated with the management plane including:

1. **Application Registration**: It includes activities like establishment of the Wave Basic Service Set (WBSS).
2. **WBSS Management**: It includes link creation activities required at the creator of the WBSS.
3. **Channel Usage Monitoring**: Monitoring channel activity is essential to select a Service Channel (SCH) to distribute the load across the service channels.

Data transmitted over wireless networks are vulnerable to a range of threats, some of which are mentioned in Section 2.2.1. The critical nature of the messages being

Length (octets)	Field			
1	protocol version			
1	type = signed			
1	signed message	signer	type=certificate	
125			certificate	
1		unsigned message	Application	ACID
1				length of ACM
10				ACM
2			message flags	
2			length of application data	
32			application data	
8			message generation time	
4			location of message transmission	latitude
4				longitude
3				elevation and confidence
28		signature	edsa signature	r
28				s

Figure 2.6: Structure of a Signed Message in IEEE 1609.2

exchanged makes their safety a vital requirement. The WAVE protocol stack aims at securing messages using the security services mentioned in the IEEE 1609.2 standard, an overview of which is given below.

2.3.4 IEEE 1609.2

The IEEE 1609.2 standard [9] defines the secure message formats and the processing required for each message to attain the desired level of security. Some of the security services provided by this standard are as follows:

1. Applications running over the IPv6 or WSMP at 1609.3 layer use the secure message formats to secure the application data.
2. The Wave Management Entity (WME) uses the secured Wave Service Information Element (WSIE) to secure the Wave Secure Announcements (WSA).

The security of safety messages is based on the Public Key Infrastructure (PKI). The source of the message (that may be encrypted) signs the hash of the message. This signed hash also known as the signature is transmitted along with the message. As distribution of all the certificates issued by a CA is impractical, the IEEE 1609.2 standard, as shown in Figure 2.6, specifies that a signed message includes the certificate of the sender containing the public key used to sign the message. The standard does not mandate the certificate hierarchy to be used however for the performance of V2V communication the OBU should possess all the root certificates required to successfully verify all the messages received.

The message generation time and location are included along with the messages to avoid replay attacks and support certificates whose validity is limited to specific geographic regions. The Application Context Mark (ACM) and Application Class Identifier (ACID) are used to identify the application generating the packet.

2.3.5 IEEE 1609.1

The IEEE 1609.1 [11] describes the key components of the WAVE system architecture. It also defines the command message formats and data storage formats to be used by applications, and specifies the types of devices that may be supported by the on board unit (OBU) resident on the vehicle.

This standard defines 3 types of applications:

1. **Resource Manager Applications** (RMA) - It is a remote entity that uses the RM to communicate with the RCP.
2. **Resource Manager** (RM) - The resource manager (or the provider) relays the messages from the RMA to the RCP. The RM provides services that allows the RMA to control interfaces present in the OBU.
3. **Resource Command Processor** (RCP) - It executes the commands given by the RMA and provides the response to the RMA via the RM.

The RMAs communicate with one or more RMs using a secured network. The RM multiplexes the communication sessions of multiple RMAs that enables each

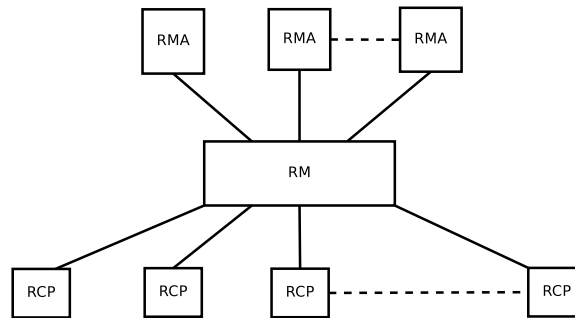


Figure 2.7: IEEE 1609.1 Modules

RMA an end-to-end communication link with RCPs. The communication is carried out to provide the RMA access to the interfaces available in the OBU as shown in Figure 2.7.

2.4 Related Work

This section provides a brief overview of related work done by the research community in the area of securing vehicular networks and modeling of vehicular communication. Section 2.4.1 provides the related work in the area of securing vehicular networks while the current work available in the area of modeling vehicular communication is available in Section 2.4.2. The related work in the area of modeling IEEE 802.11 networks in discussed in Section 2.4.3.

2.4.1 Securing Vehicular Networks

The detection of misbehaving nodes is a vital task. Once detected these nodes must be prevented from disrupting network operation. Golle *et al.* [30], propose a technique for detecting and correcting malicious data in vehicular networks by making individual nodes search for logical explanation for the data received. This is achieved by collecting information by using the sensors present on vehicles and by the information shared by the neighboring vehicles that are detected to be non-malicious. Further, the authors propose correcting the inconsistent information with those detected using the data reported by the sensors. Raya *et al.* [53], propose solutions that address the

issue of threats using a model for threat analysis. They also address implementation issues for security protocols that are suitable for vehicular networks especially in the area of authentication of nodes.

Any leak in personal information is detrimental to the anonymity of the users of vehicular networks, while authentication demands the trustworthy status of the vehicles involved. Parno *et al.* [47], study this trade-off between authentication and anonymity and propose security mechanisms that exploit the mobility and organization of vehicles on roads to address this issue.

Instantaneous dissemination of eviction information is possible if on demand connectivity exists between the security infrastructure and the entities involved in vehicular networks. Capkun *et al.* [20], address this problem for MANETs by proposing a self-organizing public-key management system that allows the users to manage (create, store, distribute, and revoke) their public keys without the help of any trusted authority (like CAs) or a fixed server. Such schemes cannot be used in vehicular networks where centralized entities like law enforcement agencies, or vehicle manufacturers *may* have a say in the revocation of certificates.

Revocation of certificates issued to malicious nodes and propagation of the information related to the revocation is vital for the success of any security system based on PKI. Jungels *et al.* [36], address the problem of revocation by proposing a set of protocols for revocation that also enables nodes to shield themselves against malicious operation. Raya *et al.* [54], extend [36] by addressing the problem of detection and eviction misbehaving nodes. The detection process is similar to the one proposed in [30], and is done by using the *K-means clustering* algorithm to single out misbehaving nodes.

In [56], Rivest discusses mechanism that could eliminate certificate revocation lists in favor of other mechanisms. The proposed mechanisms revolve around the concept of freshness that quantifies the recency of the certificate. The author asserts that the best evidence of recency is provided by frequent certificate re-issuance. The author also proposes a concept called “guaranteed period” that defines the period for which the CA *shall not* revoke the certificate. Such short term certificates, i.e.,

certificates that have a short life time, may not be practical in vehicular networks as the connectivity with the PKI for renewal of certificates within the certificate life-time cannot be guaranteed. Similar concerns that are a response to [56] for wired networks are highlighted in [41]. Goyal *et al.* [31], motivated by [56], provide an alternative to short-lived certificates. We take a similar approach in Chapter 3 to address the issue of stale revocation information in vehicular networks.

2.4.2 Modeling Vehicular Communication

In one of the primordial works of vehicular communication, Varaiya *et al.* [67], propose a system for future applications that rely on communication for improving safety and road traffic efficiency, for example, a platoon concept was proposed that relies on communication for managing vehicular traffic. Yin *et al.* [70], show that latency of DSRC is favorable for vehicular communication; they also derive *bit error rate* curves and highlight the key features of DSRC. Torrent-Morreno *et al.* [64], highlight the effects of the hidden terminal problem, existence of bi-directional links and importance of fairness while proposing applications for vehicular networks. Further, the impacts of radio propagation models using the probability of reception as a performance metric are provided in [65; 66].

In freeway scenarios occurrence of one hard braking event can many a times be followed by hard braking by vehicles in its vicinity, thus resulting in a chain of messages being generated. Yang *et al.* [69], attempt to address the issue of achieving low latency in delivering CCW messages while at the same time using the bandwidth efficiently with the help of congestion control policies that exploit the natural chain of emergency events.

In Forward Collision Warning (FCW), a member of the CCW class of applications, each vehicle (capable of vehicular communication) computes the likelihood of collision with a vehicle in front of it. ElBatt *et al.* [28], provide the latency and success probability results of the Forward Collision Warning applications and explore techniques such as broadcast rate and transmission range adaptation for improving the efficiency of broadcast messages. To address the issue of absence of retransmission of

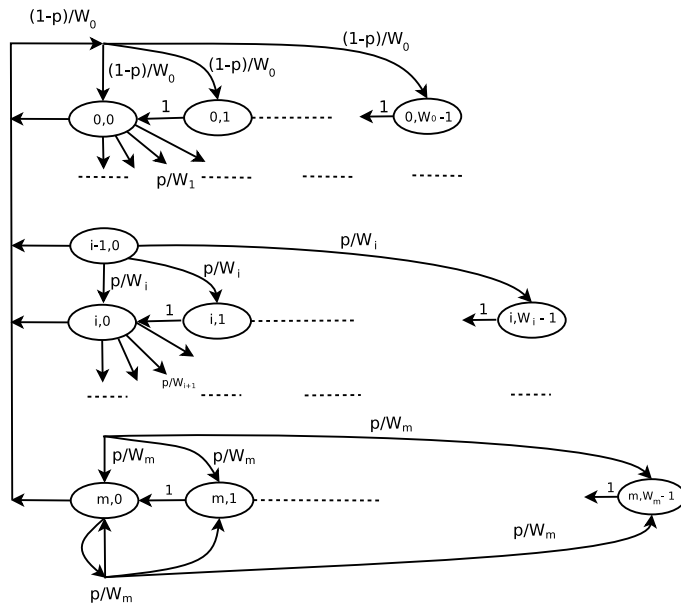


Figure 2.8: Markov Chain Model for Backoff Window Size

broadcast packets, Xu *et al.* [68], propose a scheme for retransmission of packets and provide analytical models to evaluate the performance of the proposed scheme using probability of reception failure and channel busy times as the performance metric.

2.4.3 Modeling IEEE 802.11

Performance evaluation of communication considering the impacts of security is incomplete without understanding the performance of vehicular communication without security. Thus, an understanding of the MAC layer is important for the performance evaluation of vehicular communication without security. Section 2.3.1 and Section 2.3.2 highlight the similarities between the MAC layer of the protocol stack proposed for vehicular communication and the IEEE 802.11 standard.

Modeling the back-off process of IEEE 802.11 is critical in the case of unicast communications as collisions result in retransmissions. In the seminal paper for performance analysis of 802.11 DCF, Bianchi [19] provided a Markov Chain for the back-off process to compute the saturation throughput of 802.11 DCF. Figure 2.8 shows the Markov Chain Model used to model the back-off window size assuming p

to be the probability of packet collision.

Kumar *et al.* [39], extend [19] to provide a generalized fixed point equation to obtain the collision probability for saturated MAC queues. Malone *et al.* [40], extend [19] for unsaturated MAC queues by adding new states to model the backoff when there are no packets buffered in the MAC queue. Using this model they show that the peak throughput occurs prior to saturation for unicast traffic. Similarly Chen *et al.* [21], provide a model based on the one available in [19] for broadcast traffic assuming saturated MAC queues.

Qui *et al.* [49], study the interference in wireless networks relying on broadcast and unicast communication, however they do not address any stability issues. Choi *et al.* [22], provide an analytical model to study the hidden node problem in multi-hop networks by providing a two-state Markov Chain for modeling the communication channel.

2.5 Summary

Security is an essential for safety applications like CCW. The need for robust authentication techniques has motivated the research community to propose a PKI based approach for security. The PKI based authentication relies heavily on the support of the infrastructure for obtaining the revocation information, a critical component required for authentication. Vehicular networks cannot guarantee on demand connectivity between the principals of the network and the security infrastructure thus motivating the need to quantify the security performance considering the impact of absence of on demand connectivity. Further, the proposed safety applications rely on security and broadcast communication motivating the need for studying the impact of security on the performance of broadcast communication.

In the next chapter we study the impact of intermittent connectivity between the vehicles and the security infrastructure on the security performance of vehicular networks.

Chapter 3

Performance of Security in Vehicular Networks

We now study the impact of intermittent connectivity between the principals of vehicular networks and the security infrastructure on the performance of security in vehicular networks. We propose a metric to quantify the security performance in Section 3.2. We then propose a scheme called *Freshness Checks* for accepting/rejecting packets at the security layer in Section 3.3. Modeling the security performance of the traditional Certificate Revocation Lists (CRL) based schemes and the proposed Freshness Check Scheme is presented in Section 3.4. The details of the simulations carried out for studying the security performance and the discussion of the numerical results are presented in Section 3.5

3.1 Dilemma at Receivers

Certificates issued to the principals in vehicular networks can be revoked if the certificates are compromised and/or used in malicious activities. Such malicious activities can be intentional or due to faults developed in the devices used in generating and exchanging messages in vehicular networks. In the vehicle to vehicle (V2V) context, where continuous monitoring of all the principals by the CA is a non-trivial task, the misbehavior detection is expected to be carried out by the participating vehicles in a distributed manner [54]. The various stages involved in revocation of certificates are:

1. Detection of misbehavior and/or compromise of the certificate.
2. Reporting the above event to the infrastructure (CA).
3. Revocation of the certificate(s).

In the case of revocation due to misbehavior, the CA is expected to wait for multiple reports of misbehavior of a vehicle before revoking its certificate(s). The first phase, i.e., detection of misbehavior, inevitably results in some delay in revoking the certificate of a misbehaving vehicle¹. Once the CA revokes a certificate, it is imperative for the CA to inform the other participating vehicles of this revocation.

The delays involved in detecting, reporting and dissemination of compromised certificate gives rise to a *window of vulnerability*, in which other vehicles in the network may receive messages signed using the compromised certificate whose revocation information is not yet available at the vehicles. This window of vulnerability may increase if the reporting and dissemination delays increase, and leads to a clear degradation in *security performance* of the system.

In the CRL based scheme, the revocation information is updated by adding the certificate ids to be revoked in the CRLs at the infrastructure. The CRLs at the On Board Unit (OBU) present in the vehicles can be synchronized with the CRLs at the infrastructure in many ways such as:

1. The OBU requests the latest CRL information when it contacts the infrastructure. These CRL updates can be performed by the OBU in various ways including:
 - (a) Periodic request using Cellular/WiMax links.
 - (b) Requests using Road Side Units (RSUs) or Public Safety OBUs (PSOBUs) when in communication range of such devices.
2. The infrastructure broadcasts the CRLs using FM or XM broadcasts as proposed by Jungels *et al.* [36].

On receiving a packet, the recipient checks if the certificate used is present in the CRLs in the On Board Unit (OBU). If the certificate is present in the CRLs in the OBU, then the packet can be discarded as the infrastructure considers the certificate as compromised. If the certificate is not present in the CRLs in the OBU then the recipient is faced with a dilemma as the source could be categorized as one of the following:

¹For example, Local Eviction of Attackers by Voting Evaluators (LEAVE) [54], relies on the crosschecking of evidence related to misbehavior, thus emphasizing non-avoidable detection delays.

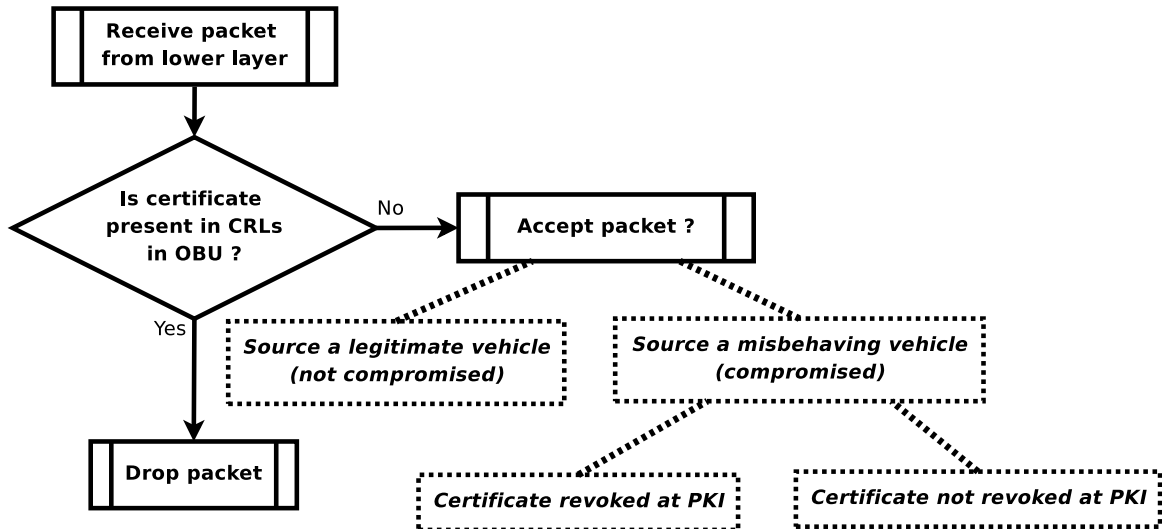


Figure 3.1: Dilemma at receivers in CRL based scheme

1. The source is a legitimate node and the certificate is not compromised.
2. The certificate is compromised and has been revoked at the infrastructure but this revocation information is not available at the OBU.
3. The certificate is compromised but the infrastructure has not revoked the certificate.

3.2 Confidence on Security Infrastructure

The mobility of the vehicles make the real time availability of CRLs a hard problem while the storage space constraints in the OBU limit the number of CRLs that can be stored. The incomplete revocation information due to the above reasons puts the recipients of messages secured using PKI in a dilemma thereby reducing the confidence with which packets are accepted/dropped. We now propose a metric, Confidence on Security Infrastructure (CoS), to quantify the confidence recipients can have on the security provided by the security infrastructure.

Confidence on Security Infrastructure (CoS): The CoS is defined as the probability that the sender's certificate has not been compromised and/or is being used for malicious activities if it is not in the CRLs available at the receiving OBU.

The CoS is dependent on

1. The freshness of the certificate [56], which specifies how recent is the certificate under consideration. This freshness complements the honest majority concept of vehicular networks [47], that assumes most of the nodes in the network are honest.
2. The number of compromised certificates that are present in the CRLs in the OBU.

When the rate of revocation r , expected inter-CRL update times ($E[T]$) and variance in inter-CRL update times $Var(T)$ is known, the CoS is given as

$$CoS = 1 - \frac{rVar(T)}{E[T]} - rE[T], \quad (3.1)$$

a proof of which is given in [50].

The following observations can be made from the above equation:

1. The CoS is independent of the rate at which the tagged vehicle comes in contact with a given vehicle using vehicular communication.
2. The CoS decreases as the expected time of CRL updates ($E[T]$) increases.
3. The CoS decreases as the rate of revocation r increases.
4. An increase in variance of the inter-update times for CRL actually decreases the CoS even for the simple system under consideration motivating the need for regular updates of CRLs.

3.3 Freshness Check Scheme

One way to increase CoS, as per Equation 3.1 is to reduce the variance of the CRL update times and, for small variance $Var(T)$, one needs small value of $E[T]$ to obtain large CoS. Since the times between CRL updates are completely determined by the mobility pattern of vehicles and availability of connectivity with the infrastructure, it is bound to be a random variable. When Road Side Units (RSUs) are used for CRL

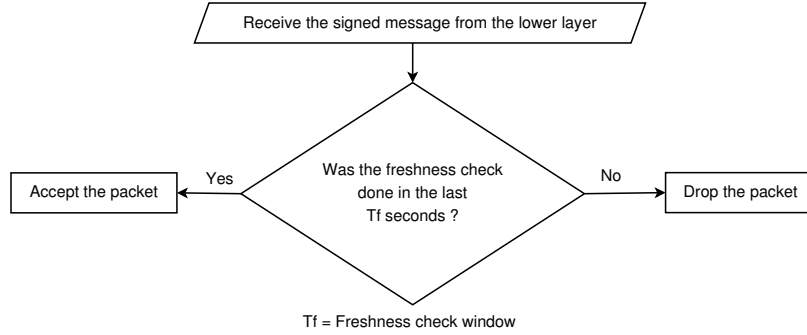


Figure 3.2: Accept/Drop mechanism in Freshness Check scheme

updates, sparse density of the RSUs in the network implies non-negligible variance in inter CRL update times.

We now propose a scheme intended to make the system behave like the one where the CRL update intervals are deterministic (resulting in $Var(T) = 0$) and small. Each node periodically performs a *Freshness Check* on its certificate. The Freshness Check is successful only if the certificate is not revoked, the details of which are provided in Section 3.3.1. On receiving a signed message, the recipient accepts the message only if the Freshness Check for the certificate was performed in the last T_f units of time². We shall henceforth refer to the window T_f as the *Freshness Threshold*.

This simple scheme is aimed at achieving a CoS that one would have obtained under zero variance ($Var(T)$) and small update times ($E[T] = T_f$). The equation for CoS in the CRL based scheme where CRL updates are performed in deterministic intervals T_f is

$$CoS = 1 - rT_f \quad (3.2)$$

which is the upper bound for the CoS achieved in the freshness check based scheme where the freshness threshold is T_f .

A small T_f is desirable as the CoS increases as T_f decreases for a given rate of revocation. Clearly, the time window T_f can not be too small as it will result in most of the messages being discarded, and shall require the OBUs to do frequent Freshness

²If the freshness was performed t_w units of time in the past ($t_w > T_f$), then packet may be accepted by tagging it the CoS corresponding to t_w . This tag can be used by the trust mechanism proposed by Raya *et al.* [52]. We do not consider such accept/drop mechanisms in our analysis

Checks. Note that the time window T_f used by vehicles determines the required rate of freshness checks by other OBUs.

3.3.1 Freshness of Certificates

The freshness of the certificate complements the honest majority principle and is aimed at addressing the following issues:

1. The safety messages have stringent latency requirements, hence the verifying time of signed messages needs to be minimized.
2. The system should minimize the time for which compromised certificate is used, i.e., reduce the window of vulnerability.
3. For the safety of the passengers, each OBU requires the safety messages generated by it to have a deep penetration and should be accepted by all the concerned entities.
4. The sender and the receiver of a signed message have an equal access to the PKI, which in the case of vehicular networks may be available at irregular intervals of time.

Each vehicle generating signed messages owns certificates signed by the CA that are valid for a finite amount of time. This certificate can be revoked for various reasons during the validity period without the knowledge of the OBU. To ensure that the recipients have confidence on the security of the message sent, the OBU can query (based on the desired CoS) to check if one of its certificates (that is still valid) is revoked. We propose adding a new field C_f in the certificate that indicates the last time a successful freshness check was carried out. The number of bits for this field shall depend on the granularity of the freshness check threshold T_f . This field initially has *the time of issue* of the certificate and is updated during subsequent Freshness Checks. A Freshness Check is performed by the OBU by sending a signed message to the PKI indicating Freshness Check Request and the certificate whose validity is to be confirmed by the CA. The following steps are carried out at the Security Infrastructure (CA) during the Freshness Check operation:

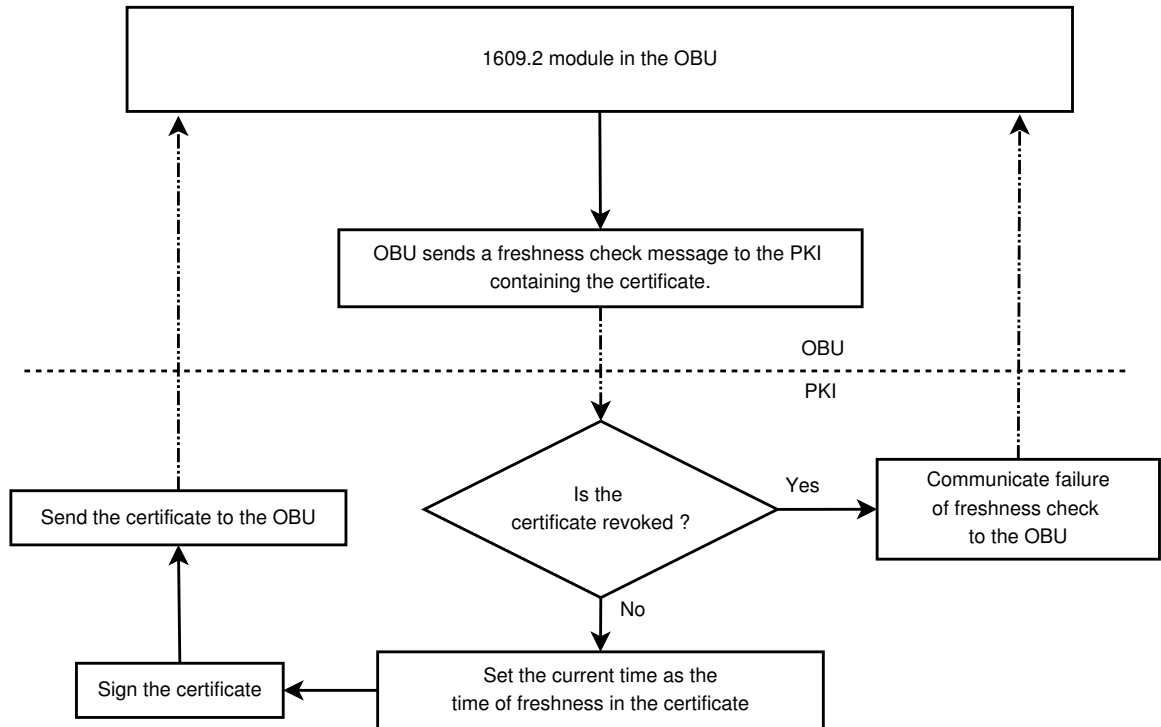


Figure 3.3: Operations during Freshness check

1. If the certificate is not revoked then set the freshness check time in the certificate to the current time else set the freshness check time to 0, indicating the revocation of the certificate.
2. Sign the certificate with the private key of the CA.

This is fundamentally different from issuing new certificates and the concept of short-lived certificates (where certificates are valid only for a finite amount of time) as:

1. New keys are not being generated, hence the time involved in generating a fresh pair of Public and Private keys is avoided.
2. The other fields of the certificate are not modified or generated by the CA and credentials need not be provided to the CA for verification of the data present in the certificate as the certificate is valid during the time of the Freshness Checks.
3. The expiry time of certificate remains the same as new keys are not generated, hence the effective time for which the certificate can be used is from the time of freshness check or issue (which ever is the latest) to the expiry time.

3.3.2 Advantages and Disadvantages of Freshness Checks

The *advantages* of having a freshness field in the certificates can be listed as follows:

1. The receiving OBU accepts or drops messages based on the freshness of the certificate, hence the time of verifying the message is *constant* and is *independent of the number of revoked certificates*.
2. The OBU need not store the CRLs. This *reduces the storage space* required in the OBUs and can nullify the problem of distribution of CRLs.
3. Without Freshness Checks, the time for which a compromised node can cause chaos is the average CRL update time, however with Freshness Checks the operating time is now limited to T_f (the freshness check threshold) which is independent of the rate at which the other nodes communicate with the infrastructure.
4. When the Freshness Check of certificate fails, due to reasons beyond the control of the OBU, the OBU can stop using the certificate thus *reducing the number of messages signed by revoked certificates*.
5. The validity of short-lived certificates is limited, while in the case of Freshness Checks, the certificate can be valid for longer durations and based on the required *CoS*, the OBU receiving signed messages *can decide the T_f* (or PKI can advertise this value) to accept/drop the message.

The *disadvantages* of above scheme can be listed as follows:

1. For all practical reasons the freshness check threshold (T_f) cannot be less than the average freshness check interval (T_c). Hence, for a given value of T_c that is dependent on the availability of connectivity with the infrastructure. If Freshness Check requests are routed via RSUs, then the mobility model and the number of RSUs present in a geographical region control T_c , and for a given T_c , the *CoS* decreases as the rate of revocation increase.
2. The Freshness Checks increase the computational requirements of the infrastructure as certificates are signed each time a Freshness Check is performed by a principal.

3.4 Modeling Security Performance

This section discusses the analytical model developed to study the security performance of the CRL based scheme and the Freshness Check scheme in vehicle-to-vehicle (V2V) networks. This effort becomes even more important when one realizes that the large number of random variables in this system are detrimental to the scalability of the simulations. We now discuss some of the factors that affect security performance, and at the same time pose various decision problems, as listed below.

1. *V2V service penetration*: Higher spatial density of V2V equipped vehicles could result in speedy detection of misbehavior, and may also imply higher rate of vehicles misbehaving.
2. *Revocation rate*: The revocation rate affects the security performance, while the security performance in turn might affect the revocation rate. High rate of certificate revocation may lower security performance. Thus, the rate at which certificates are revoked, for example 5% [58] in the Internet, is a very critical parameter.
3. *Revocation information dissemination scheme*: This could either be explicit, like Certificate Revocation Lists (CRLs), or implicit, like in Freshness Checks. Each of these schemes have their own processing, storage and communication overheads that can affect the security performance.
4. *Uplink and Downlink interface between vehicles and CA*: Various technologies can be used for Vehicle→CA communication (uplink), for example, DSRC (via RSEs), home WiFi, Cellular link etc. Further, technologies like DSRC (via RSEs), cellular link, XM broadcast, FM broadcast etc., can be used for CA→Vehicle communications (downlink). Uplink and downlink choices may be coupled, for example, XM or FM downlink must be accompanied by an alternative uplink technology, thus implying additional cost. *These choices determine the delay in detection of misbehavior and dissemination of revocation information.*
5. *Node eviction scheme*: It is possible that the CA may remotely deactivate

Status of Packet Source	Action taken by Receiver	Characterization of Packet
Legitimate	Accept	True Positive
Misbehaving	Reject	True Negative
Misbehaving	Accept	False Positive
Legitimate	Reject	False Negative

Table 3.1: Characterization of packets.

the message signing functionality of the revoked vehicle [54] or in the case of Freshness Checks invalidate the certificate by setting the field indicating the last Freshness Check time of the certificate to 0. Remote deactivation can be modeled as a revocation information broadcast using FM or XM, hence, one need not consider this option separately while studying security performance.

To understand the dependence of security performance on the factors mentioned above, we carry the following analytical modeling exercise. This analysis is useful in *comparing different systems* (various uplink and downlink options, information dissemination scheme etc.) with respect to their communication/storage/processing requirements when trying to decide on various available options.

We consider a tagged node that moves in a given area and exchanges messages with m other (initially legitimate) mobile nodes. All the nodes have statistically the same mobility pattern. We assume that certificates get revoked only due to malicious behavior exhibited by the principals in the vehicular network. Further, we assume *no correlation* between the malicious behavior of the nodes and that the malicious behavior does not result in any modification of packet generation; this may not be true for all malicious activities. All the m nodes eventually start misbehaving resulting in the revocation of their certificates. We assume connectivity with the infrastructure is available via access points, for example RSEs, and vehicles *may* communicate with the security infrastructure (CA), whenever they come in the communication range of these access points. On contacting the CA, in the CRL based scheme, the On Board Unit (OBU) of each vehicle independently updates its CRLs, while in the freshness check based scheme, the OBU independently updates the freshness information of

its certificate. In the CRL based schemes the packets from nodes whose certificates are present in the CRLs at OBU are dropped, rest all packets are accepted, while in the freshness check based scheme only those packets signed using fresh certificates, i.e., whose freshness check was done in the last T_f units of time (T_f represents the freshness threshold) are accepted. The accept/drop mechanisms at the security layer may have packets that can be characterized as one entry in Table 3.1.

The following terms are used in the analysis of CRL based schemes and Freshness Check scheme.

$L_m(\cdot)$ represents the distribution function of time intervals between successive receptions of a message from a given node to the tagged node. We assume periodic message generation by the nodes resulting in $L_m(\cdot)$ to be exponential based on our simulation results presented in Section 3.5, and the results obtained by Groenevelt *et al.* [32] for the random walker and random direction mobility models in a *bounded domain*.

$\lambda(m) = \frac{1}{\int x dL_m(x)}$ denotes the message reception rate by the tagged vehicle from one of the other vehicles.

$I(\cdot)$ represent the distribution function of time intervals between successive contacts with the CA. We assume that the infrastructure points are available after fixed time intervals. Each time a node comes in communication range of the access points, it probabilistically communicates with the infrastructure. Henceforth, we assume $I(\cdot)$ to be exponential.

$c = \frac{1}{\int x dI(x)}$ gives the rate at which the nodes communicate with the infrastructure. *This quantity (c) can be used to abstract the infrastructure density, the frequency of vehicle \leftrightarrow CA communication (and hence the involved communication costs), and the security rewards involved in communicating with the infrastructure.*

$R(\cdot)$ denotes the distribution of time between successive revocations which is independent of the number of un-revoked certificates at the time instant of revocation.

$r = \frac{1}{\int x dR(x)}$ represents the revocation rate.

$X^{(j)}(\cdot)$ represent the j -fold convolution of distribution $X(\cdot)$.

$\tilde{X}(\cdot)$ represent the excess distribution of $X(\cdot)$.

We use the following two approaches to analyze the impact of revocation rate on the security performance:

1. A node-centric model of faulty sensors. This model provides a lower bound on the infrastructure requirements (vehicle \leftrightarrow CA communication) for a desired security performance. Further, we assume that the life-time of these devices, i.e. time after which these devices become faulty, is sampled from an exponential distribution i.e, $R(\cdot)$ is exponential.
2. A given system-wide misbehavior rate which is independent of the node density to incorporate malicious activities. We assume the smallest time interval between any two nodes to start misbehaving intentionally is sampled from an exponential distribution due to an intuitive lack of intentional malicious activities.

3.4.1 Performance of CRL Based Schemes

In the CRL based schemes, the tagged node assumes that the certificate of the source of a received message is not revoked if and only if it is not present in its copy of the CRLs. Thus, there are no False Negatives, however False Positives are possible due to delays in receiving the eviction information.

We assume that the certificate(s) issued to a node are revoked at the time instant at which the node starts misbehaving. Assume that the certificate issued to node i gets revoked at time t_r . All the packets received from node i in the time interval $(0, t_r)$ are categorized as True Positives. Let $t_u > t_r$ represent the time of the first CRL update by the tagged node after node i starts misbehaving. All the packets received from the tagged node after time t_u are rejected as the tagged node is in possession of

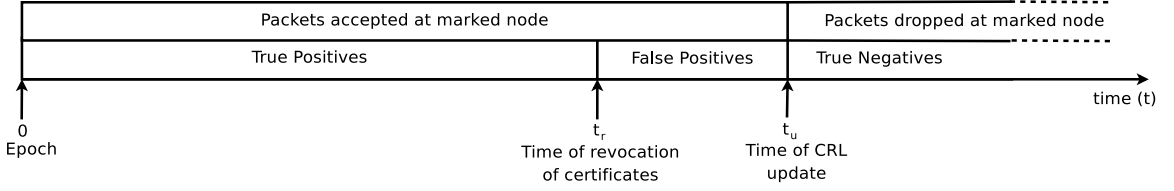


Figure 3.4: Categorization of packets in CRL based schemes

the revocation information³ of node i , hence, these packets are categorized as True Negatives. All packets received by the tagged node from vehicle i in the time interval (t_r, t_u) are False Positives.

When $TP(t)$ and $FP(t)$ represent the number of True Positives and False Positives accepted by time t , the CoS for the CRL based schemes can be given as

$$CoS = \frac{TP(t)}{FP(t) + TP(t)} \quad (3.3)$$

3.4.1.1 Misbehavior by Faulty Nodes

In the node-centric model where the misbehavior of a vehicle is attributed to it sending incorrect data only due to faults developed in the OBU (and the attached sensors, data aggregation schemes, etc.), the lifetime (reliability) of the OBU determines the time for which the vehicle is not misbehaving. We do not assume any correlation between the faulty behavior of the vehicles, hence, each vehicle can be studied in isolation.

Let $FP(i)$ denote the expected number of False Positives from node i which starts misbehaving at time instant t_r . The first time instant $t_u > t_r$, at which the tagged node does a CRL download is assumed to contain the certificate of vehicle i . The probability that the tagged node received *at least* j packets ($j \geq 1$) in the time interval (t_r, t_u) is then⁴ $L_m^{(j)}(t_u - t_r)$.

³We are assuming that the first CRL download by the tagged vehicle after start of *misbehavior* of vehicle i declares the node i to be *revoked*. This is an assumption expected to provide an upper bound on the security performance. The analysis presented here can easily be extended to incorporate different phases like detection, reporting and dissemination. However the qualitative nature of the results are expected to remain unchanged.

⁴As we assume $L_m(\cdot)$ to be exponential, we currently do not account the residual first-inter-message time after t_r .

Thus the *expected number* of False Positives from node i , $FP(i)$, can be given as

$$FP(i) = \int_{y=0}^{\infty} \left[\sum_{j=1}^{\infty} L_m^{(j)}(y) \right] dI(y) \quad (3.4)$$

As we assume $L_m(\cdot)$ and $I(\cdot)$ to be exponential, we get

$$FP(i) = \frac{\lambda(m)}{c} \quad (3.5)$$

The True Positives from node i are the packets received by the tagged node till the node i becomes faulty at time t_r . The expected number of True Positives received by tagged node from vehicle i given that it received j packets ($j \geq 1$) in the interval $(0, t_r)$ is then

$$TP(i) = \int_{y=0}^{\infty} \left[\sum_{j=1}^{\infty} L_m^{(j)}(y) \right] dR(y). \quad (3.6)$$

Again as we assume the life-time of the vehicles to be sampled from an exponential distribution, we get

$$TP(i) = \frac{\lambda(m)}{r} \quad (3.7)$$

The absence of correlation between the faulty behavior of the vehicles allows us to study each node in isolation. Thus, the CoS for the CRL based scheme when misbehavior is due to faults developed can be given as

$$\begin{aligned} CoS &= \frac{TP(i)}{TP(i) + FP(i)} = \frac{\frac{\lambda(m)}{r}}{\frac{\lambda(m)}{r} + \frac{\lambda(m)}{c}} \\ \therefore CoS &= \frac{c}{c + r} \end{aligned} \quad (3.8)$$

The independence of CoS with respect to $\lambda(m)$ implies that CoS does not depend on the number of nodes and rate of generating packets⁵. This observation is confirmed by our simulation analysis presented in Section 3.5.

⁵The rate of inter-meetings, $\lambda(m)$ can be abstracted as packet generation rates

3.4.1.2 Misbehavior due to Maliciousness

We now assume misbehavior is due to intentional malicious behavior exhibited by the nodes. Let $R(\cdot)$ denote the distribution of time between successive starts of misbehavior; at such an instant, one of the legitimate vehicles is chosen at random as the misbehaving vehicle⁶. We assume $R(\cdot)$ to be exponential because of the intuitive lack of correlation between malicious behavior of the nodes. Thus, the time instant at which the k -th vehicle starts of misbehaving is obtained by the k -fold convolution of the Erlang distribution $Er_m(\cdot)$, with a probability $\frac{1}{m}$ for $1 \leq k \leq m$, resulting in revocation instants being sampled from the distribution

$$R_m(u) = \sum_{k=1}^m \frac{1}{m} Er_m^{(k)}(u). \quad (3.9)$$

To get the expected number of True Positives from node i , the k^{th} node to be revoked, we need to condition on the time instant at which a vehicle starts misbehaving. The expected number of True Positives from node i can be given as

$$\begin{aligned} TP(i) &= \int_{u=0}^{\infty} \left[\sum_{j=0}^{\infty} L_m^{(j)}(u) \right] dR_m(u) \\ \therefore TP(i) &= \sum_{k=1}^m \frac{1}{m} \int_{u=0}^{\infty} \left[\sum_{j=0}^{\infty} L_m^{(j)}(u) \right] dEr_m^{(k)}(u). \end{aligned} \quad (3.10)$$

As we assume $L_m(\cdot)$ to be exponential with a mean $\lambda(m)$, and $\frac{1}{r} = \int x dR_m(x)$ is the time between the successive starts of misbehavior, we get

$$TP(i) = \sum_{k=1}^m \frac{\lambda(m)k}{rm} = \frac{(m+1)\lambda(m)}{2r} \quad (3.11)$$

The False Positives from any node i , can be given by Equation 3.5. Thus, the CoS is given by

$$CoS = \frac{TP(i)}{FP(i) + TP(i)} = \frac{c * (m+1)}{2r + c * (m+1)} \quad (3.12)$$

⁶Once a node starts misbehaving, it never stops misbehaving.

3.4.2 Performance of Freshness Check Scheme

We now assume that only Freshness Checks are performed by the participating vehicles. The accept/drop algorithm at the tagged vehicle is to check whether the sender has done a freshness check in last T_f time units. One can extend this *hard* acceptance/drop scheme by tagging a packet with a probability that depends on the time elapsed since the sender did the last freshness check. This probability distribution can then be used to assist the in accept/drop decision, or could be used to arrive at *trust* assignment for the scheme proposed in [52]. The analysis presented in this section can be extended to such scenarios. The Freshness Check scheme can introduce False Negatives if a legitimate node has not done freshness check in time interval T_f ; CRL based schemes do not introduce such False Negatives.

Further, we need to understand the impact of parameter T_f on the security performance of this system. As freshness checks involve signing of certificates by the certifying authority (CA) after modifying the freshness field in the certificate, a large value of T_f implies low certificate signing frequency (for the CA), while this results in increased False Positives. Further, small value of T_f increases the load on certifying authority (CA), and at the same time increasing the False Negatives.

3.4.2.1 False Positives

The Freshness Check scheme proposed in Section 3.3 requires each node to periodically check the status of its certificate. If the certificate is revoked, then it is expected that the revocation information of the certificate, present in the field containing the last time of freshness checks, is updated in the OBU. Faults developed in the OBU can result in the failure of updating new certificates, hence for our analysis we consider two cases of False Positives mentioned below:

1. Freshness Checks are not performed after the nodes start misbehaving or the certificates updated after Freshness Checks are not installed after the nodes start misbehaving resulting in the field containing the last Freshness Check time in the certificates *not getting updated* after the Freshness Check operations are

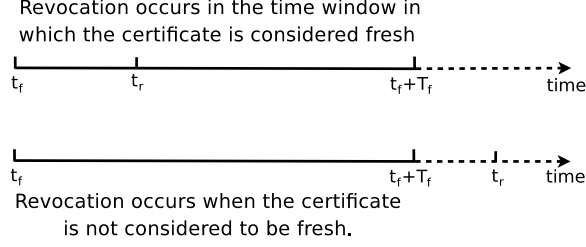


Figure 3.5: Possible instants of revocation in Freshness Check Scheme.

performed. Thus, the time window in which the packets are accepted depends only on the Freshness Check Threshold (T_f).

2. The field containing the last Freshness Check time in the certificates is updated by the Freshness Check operations performed after revocation. Thus, the time window in which packets are accepted depends on the Freshness Check threshold T_f and the rate of performing Freshness Checks.

We shall now consider the case where the field containing the Freshness Check time is not updated by Freshness Check operations performed after revocation. Let t_f denote the time of the last Freshness Check operation performed before the i -th node is revoked at time t_r . All the packets in the time window (t_f, T_f) are accepted. If $t_f \leq t_r \leq t_f + T_f$, then the packets accepted in the time interval (t_r, T_f) result in False Positives. If $t_r > t_f + T_f$, then none of the packets accepted in the time window (t_f, T_f) can be categorized as False Positives. Let V_r denote the time for which the Freshness Check is valid after revocation. As $R(\cdot)$ represents the distribution of the time between successive revocation and as we assume exponential inter-infrastructure meeting times with a mean $1/c$, $P(V_r > v) = 0$ when $v \geq T_f$ and when $v < T_f$

$$\begin{aligned}
 P(V_r > v) &= \int_{tr=T_f-v}^{\infty} 1 - e^{-c(T_f-v)} dR(t_r) + \int_{tr=0}^{T_f-v} dR(T_f - v) \\
 \therefore P(V_r > v) &= e^{-c(T_f-v)} R(T_f - v) + [1 - e^{-c(T_f-v)}],
 \end{aligned}$$

Thus, the total number of False Positives from node i can be given as

$$FP(i) = \lambda(m) \int_{v=0}^{T_f} e^{-c(T_f-v)} R(T_f - v) + [1 - e^{-c(T_f-v)}] dv. \quad (3.13)$$

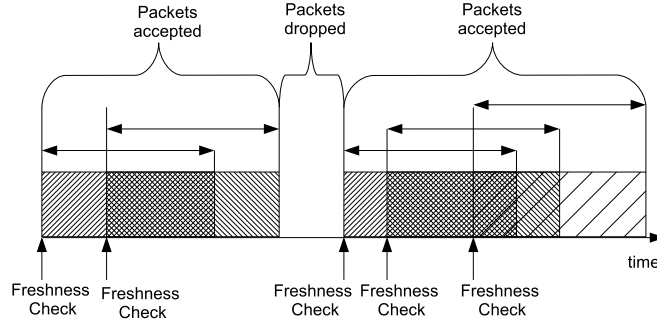


Figure 3.6: False Negatives as Idle Periods of $G/D/\infty$ queue.

When certificates are updated after Freshness Check operations performed after revocation, then if F_r represents the time to perform the freshness check after revocation, then the time for which the packets are accepted after revocation A_r is

$$A_r = \min(F_r, V_r)$$

$$\therefore P(A_r > v) = P(F_r > v)P(V_r > v) = e^{-cv}(e^{-c(T_f-v)}R(T_f - v) + 1 - e^{-c(T_f-v)})$$

Thus, the total number of False Positives from the i -th node when Freshness Checks results in updated revocation information after the revocation of the i -th node is

$$FP(i) = \lambda(m) \int_{v=0}^{T_f} e^{-cv}(e^{-c(T_f-v)}R(T_f - v) + 1 - e^{-c(T_f-v)})dv. \quad (3.14)$$

3.4.2.2 False Negatives

False Negatives are possible only when a legitimate node's message is discarded because of its failure to perform a freshness check. Figure 3.6 shows that the False Negatives can be modelled as the packets sent during the idle period of the corresponding $G/D/\infty$ queue. As we assume that the time between successive vehicle \leftrightarrow CA communications is exponential, we get an $M/D/\infty$ model. As we assume the inter-meeting times between the nodes to be exponential we get $FN(t; m) = TI(t; m)\lambda(m)$, (where $FN(t; m)$ represents the false negatives till time t when there are m nodes present in the system). Here $TI(t)$ is the expected amount of time an $M/D/\infty$ queue is idle till time t , the time at which node i is revoked, given that it started in steady state at

time 0.

The busy period distribution for an $M/D/\infty$ queue with customer arrival rate f and service requirement T_f , (as per [60, Equation 4]), has a jump of height e^{-fT_f} at T_f , and on (T_f, ∞) has density

$$h(t) = \sum_{k=0}^{\lfloor \frac{t}{T_f} \rfloor - 1} (-1)^k \frac{(fe^{-fT_f})^{k+1}}{k!} [(t - (k+1)T_f)^k - e^{-fT_f}((t - (k+2)T_f)^+)^k]. \quad (3.15)$$

Let $H(\cdot)$ represent the distribution function of the busy period and $\tilde{H}(\cdot)$ its excess distribution. We can find $TI(\cdot)$ in the following manner. Let

$TI_0(x)$ be the expected time spent in idle period till time x given that an idle period *is going on at time 0*.

$TI_1(x)$ be the expected time spent in idle period till time x given that a busy period *has just started at time 0*.

P_0 be the steady state probability that the system is idle.

Then, we can write down the following renewal-type equations.

$$TI(t) = P_0 t e^{-ft} + P_0 \int_{y=0}^t [y + TI_1(t-y)] f e^{-fy} dy + \int_{y=0}^t TI_0(t-y) d\tilde{H}(y), \quad (3.16)$$

where

$$TI_1(t) = \int_{y=0}^t TI_0(t-y) dH(y), \quad (3.17)$$

$$\text{and } TI_0(t) = t e^{-ft} + \int_{y=0}^t [y + TI_1(t-y)] f e^{-fy} dy. \quad (3.18)$$

True Positives: The total number of packets transmitted by a node to the tagged node is independent of the dissemination scheme as it depends on the transmissions till the node starts misbehaving. Thus the true positive performance of the freshness check scheme is obtained by deducting the False Negatives from the True Positives for the CRL-based scheme. *This implies that the true positives are lower in case of freshness check based scheme.*

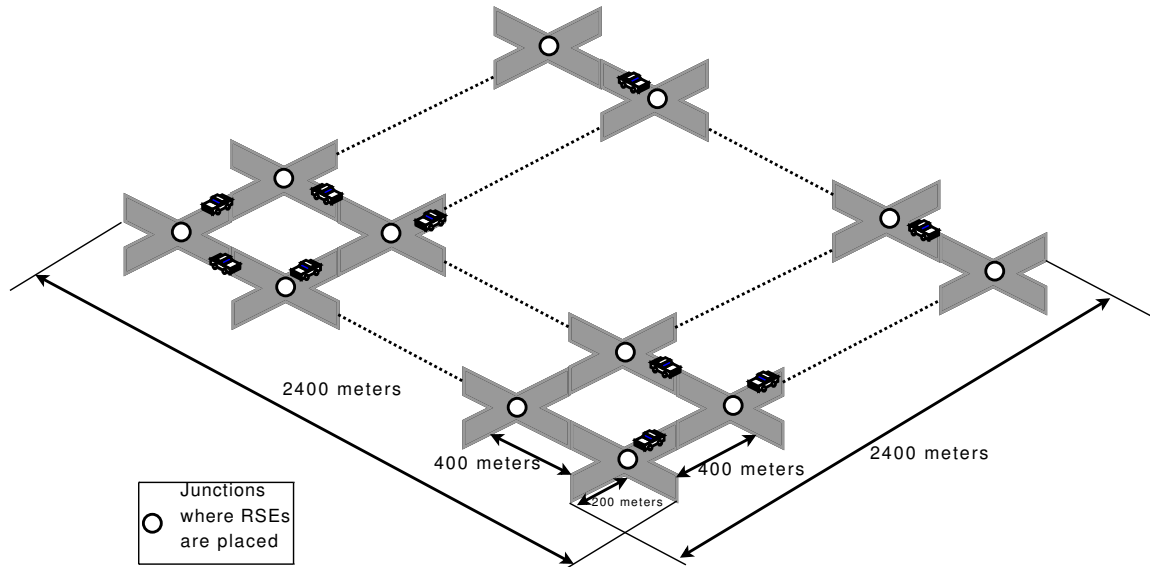


Figure 3.7: Topology used in simulations.

3.5 Numerical Results

We performed simulations using the ns2 simulator [3], in which m vehicles and a tagged vehicle followed the mobility model provided by Bai *et al.* [17], over a Manhattan grid of $2400\text{ meters} \times 2400\text{ meters}$ with a maximum velocity of 20 m/sec . The transmission range of the OBUs on each vehicle was set to 150 meters [15]. The wireless protocol used at the MAC layer was IEEE 802.11 and the Free Space model was used for wireless propagation. Packets were broadcasted once every 100 ms [15], by each of the vehicles, and all the m vehicles eventually became malicious. We assumed that misbehavior either due to devices becoming faulty or by intentional malicious activities did not result in any change in packet generation rates. Connectivity with the infrastructure was provided at regular intervals via Road Side Entities (RSEs) placed at every junction, as shown in Figure 3.7. Each time a vehicle came in communication range of the RSEs⁷, it communicated with the infrastructure with a given probability. *This probability abstracts the infrastructure density, the involved communication costs, and the security rewards involved in communicating with the infrastructure.*

⁷RSEs contain the Road Side Unit

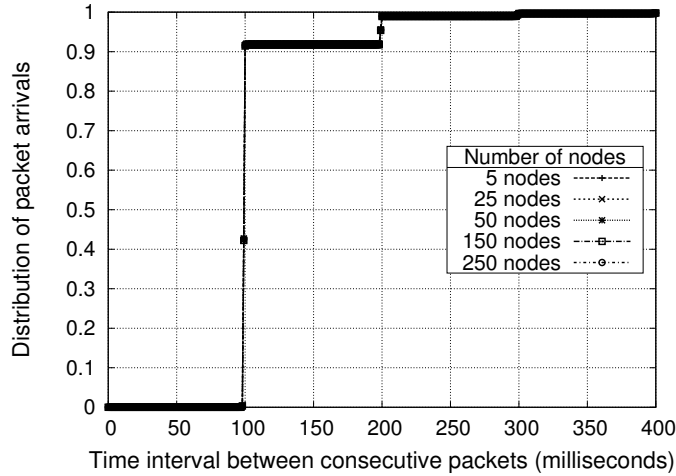


Figure 3.8: Inter-meeting times.

The *mean time* between RSE meetings was found to be approximately 35 seconds. Figure 3.8 gives the distribution of inter-packet arrival times at the marked node from the other m nodes. We observe this distribution to be *lighter than exponential*. This observation is not new, as inter-meeting times have been shown to be exponential for the random walker and random direction mobility models in a *bounded domain* by Groenevelt *et al.* [32].

Note that *the quantitative values used are only for illustrations* as we are currently interested only in the qualitative behavior. The simulations were time consuming as we had to take an average of approximately 50 thousand random sample paths (up to 1000 revocation sample paths depending on m that was varied from 5 to 250, and 50 mobility sample paths for each revocation sample path), thus justifying the analytical approach needed to address this problem.

3.5.1 Performance of CRL based schemes

In the CRL based scheme, the marked node performs CRL updates with a probability P_u each time it comes in the communication range of the RSEs, thus, resulting in $35/P_u$ as the mean time interval between successive CRL updates. Another way to look at this system is that a vehicle encounters an RSE at a junction with probability P_u , thus P_u can be used to obtain the desired the spatial RSE density. The tagged node

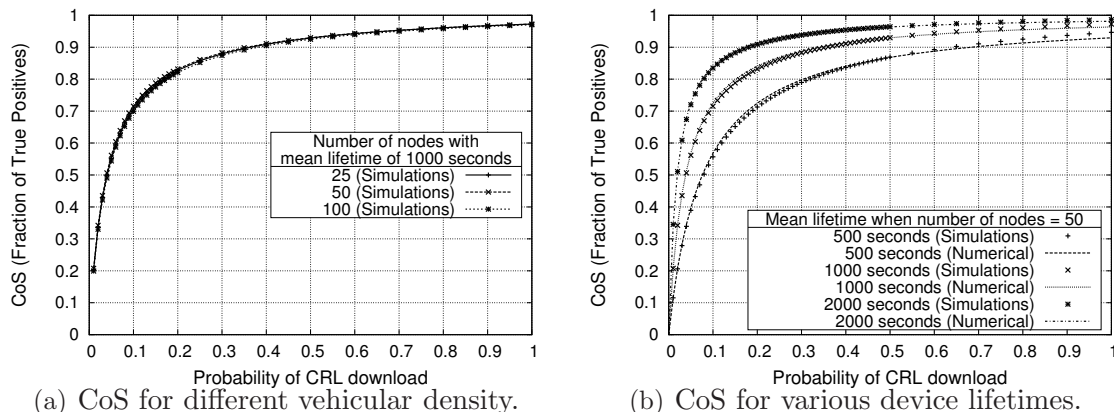


Figure 3.9: CoS when revocation occurs due to faults in devices.

discards all the messages from a vehicle whose revocation information is available at the marked node. However, due to possible delay in receiving this information, the tagged vehicle may accept some messages from a vehicle that has recently started misbehaving. Note that we are currently not talking about a local node eviction schemes such as LEAVE [54], where nodes reject packets from nodes detected as misbehaving.

3.5.1.1 Misbehavior by Faulty Nodes

When misbehavior is only due to devices becoming faulty, Figure 3.9(a) shows that the CoS is independent of the number of nodes (m) while Figure 3.9(b) shows that CoS is *dependent on the rate at which each of the vehicles starts misbehaving*. Further, Figure 3.9(b) shows that the CoS is a concave function of P_u and also depicts the existence of a *knee* with respect to P_u , i.e., we observe CoS is almost insensitive to P_u beyond a particular value of P_u . Clearly, the knee shifts right as the *revocation rate increases*. These observations can be interpreted in the following ways:

1. The infrastructure must ensure that P_u , that abstracts the rate of disseminating revocation, information is above the knee. The value of P_u should be kept as small as possible as P_u also represents the rate of communication with the infrastructure and/or infrastructure deployment costs.

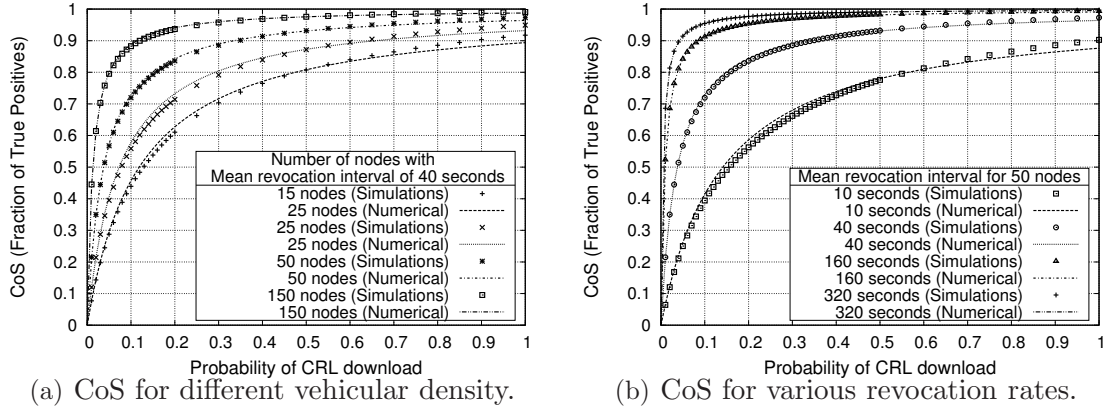


Figure 3.10: CoS when revocation is due to intentional misbehavior.

2. The rate of communicating with the infrastructure need not scale up as the V2V penetration increases as Figure 3.9(a) shows that the CoS is insensitive to the number of V2V equipped vehicles. Thus, a fixed number of RSEs that are initially deployed should suffice when misbehavior is only due to faults.

3.5.1.2 Misbehavior due to Maliciousness

To simulate misbehavior due to intentional malicious behavior we assumed inter-revocation times to be exponential due to intuitive lack for reasoning misbehavior. Figure 3.10(a) and Figure 3.10(b) show that the CoS depends on the rate of revocation and the node density. These observations can be interpreted in the following ways:

1. The rate of communication (P_u) between the nodes and the infrastructure should increase as the density of V2V enabled vehicles increase for maintaining a desired level of CoS. Equation 3.12 can be used to calculate this rate of communication.
2. The density of V2V enabled nodes affects the CoS, hence the arrival process of new nodes plays a vital role in this system. If P_u is kept to the minimum to control the costs, the infrastructure may be required to update the nodes on the desired rate of communication for the current node density.

3.5.2 Performance of Freshness Check Scheme

In the freshness check based scheme, the m nodes perform freshness checks with a probability P_f whenever they come in contact with the RSEs. The tagged node *discards* messages from vehicles that have not performed freshness checks in the last T_f units of time. As Freshness Checks result in False Negatives, the fraction of True Positives was computed as $\frac{TP}{TP + FP + FN}$, where TP, FP, and FN respectively denote the number of True Positives, False Positives, and False Negatives. The False Negatives till time t were computed as the total time for which the $M/D/\infty$ queue was idle till t . Figure 3.11 gives the evolution of the idle times for different values of P_f , the probability of performing Freshness Check operation when in communication range of RSEs, and T_f , the Freshness Check Threshold.

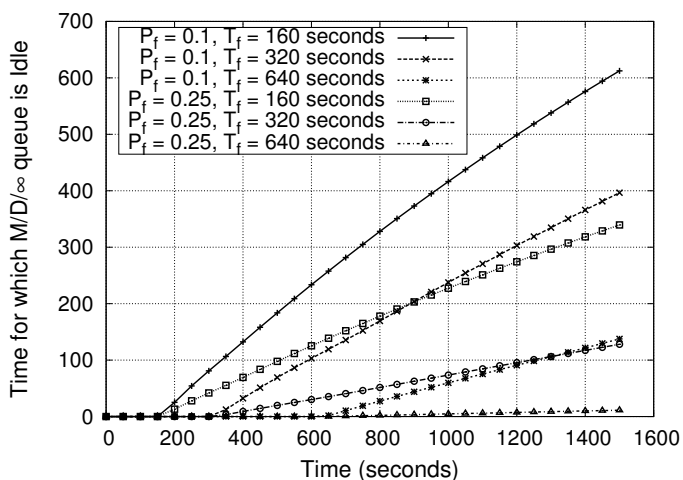
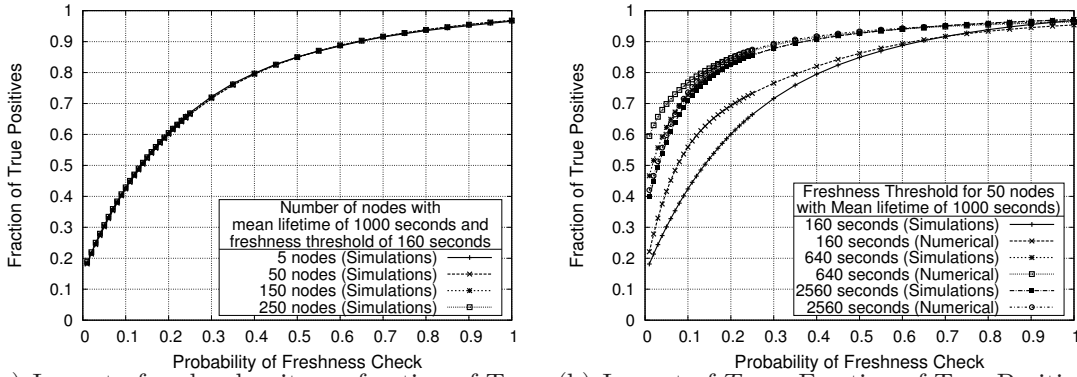


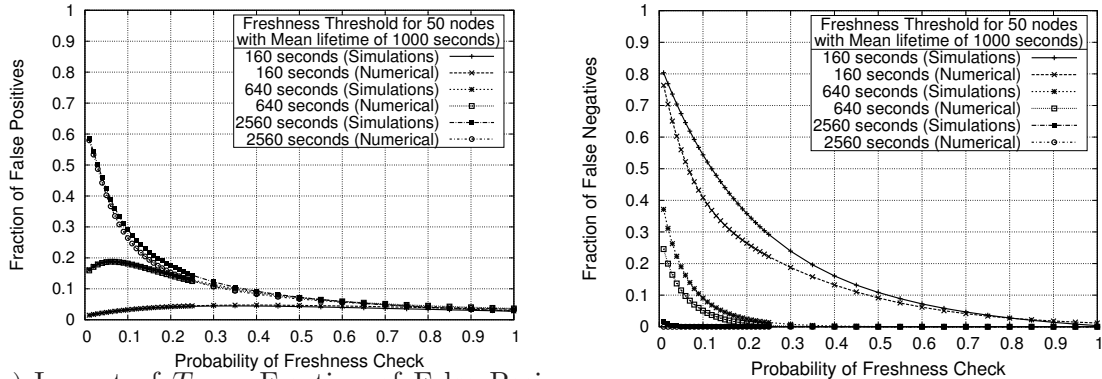
Figure 3.11: Evolution of the time for which a $M/D/\infty$ queue is idle.

3.5.2.1 Misbehavior by Faulty Nodes

When misbehavior is only due to devices becoming faulty, Figure 3.12(a) shows that the fraction of True Positives is independent of the number of nodes (m). The true positives for the Freshness Check scheme were numerically calculated by subtracting the False Negatives from the total number of True Positives in the corresponding CRL based scheme for the given value of m and r . Thus, as the accept/drop mechanism of



(a) Impact of nodes density on fraction of True Positives. (b) Impact of T_f on Fraction of True Positives.



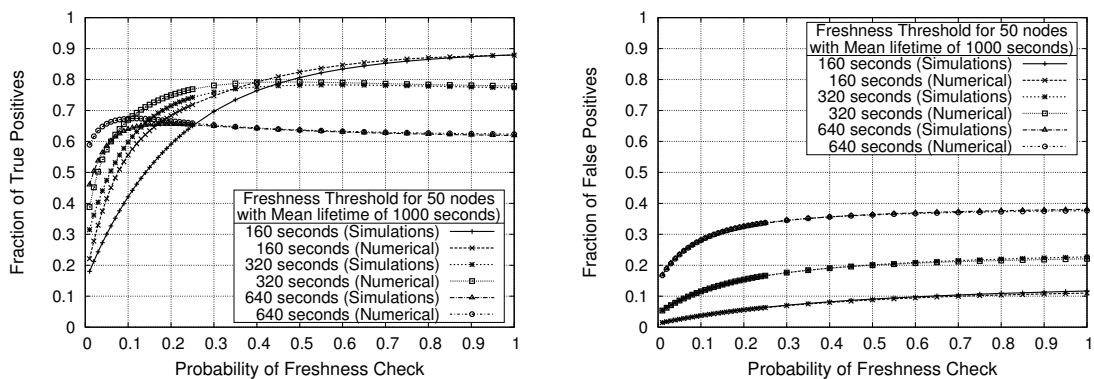
(c) Impact of T_f on Fraction of False Positives. (d) Impact of T_f on Fraction of False Negatives.

Figure 3.12: Impact of node density and Freshness Check Threshold in Freshness Check Scheme when revocation occurs due to faults.

the Freshness Check Scheme results in False Negatives the fraction of true positives *may* be lower than those obtained in the CRL based schemes.

For a given rate of performing Freshness Checks, which is controlled by P_f , increasing T_f results in a reduction in False Negatives as shown in Figure 3.12(d). However, increasing T_f results in an increase in False Positives as shown in Figure 3.12(c). Thus, Figure 3.12(b) shows that an increase in T_f , (when $P_f = 0.1$), from 160 seconds to 640 seconds results in an increase in the fraction of True Positives as the fraction of False Negatives start decreasing while a further increase in T_f to 2560 seconds results in an increase in False Positives thus reducing the fraction of True Positives.

In the simulations whose results were presented in Figure 3.12 we assumed that the certificate modified after Freshness Checks is successfully installed in the On Board



(a) Impact of T_f on Fraction of True Positives. (b) Impact of T_f on Fraction of False Positives.

Figure 3.13: Impact of T_f in Freshness Check scheme when revocation occurs due to faults (Certificate revocation information not updated).

Unit (OBU) after the Freshness Check, thus, Figure 3.12(a) and Figure 3.12(b) show that increasing the rate of performing freshness checks (which is given by P_f) increases the fraction of True Positives. However, due to the faults if the certificates are not updated or the Freshness Check operation is not performed after the devices become faulty then as P_f increases then the False Positives increases as the probability of performing the Freshness Checks close to the time of revocation increases. The impact of T_f in such a system where the Freshness Checks do not guarantee installation of the rejected certificate in the OBU are given in Figure 3.13. The fraction of False Positives increases as P_f increases as shown in Figure 3.13(b) which is in stark contrast to what we observed in Figure 3.12(c). Thus, in Figure 3.13(a) for $T_f = 640$ we observe that an increase in P_f results in a drop in the fraction of True Positives.

The impact of the revocation rate r (inverse of the device lifetime), when nodes update and do not update their certificates on Freshness Checks performed after revocation, on the Freshness Check scheme is given in Figure 3.14. The True Positives initially increase (at $P_f = 0.1$) as the life time decreases from 1000 seconds to 500 seconds. This is because the decrease in the device lifetime results in a decrease in the time spent idle in the $M/D/\infty$, thus reducing the fraction of False Negatives as shown in Figure 3.14(e) and Figure 3.14(f). The False Positives are controlled by the rate of communication with the infrastructure and the Freshness Threshold,

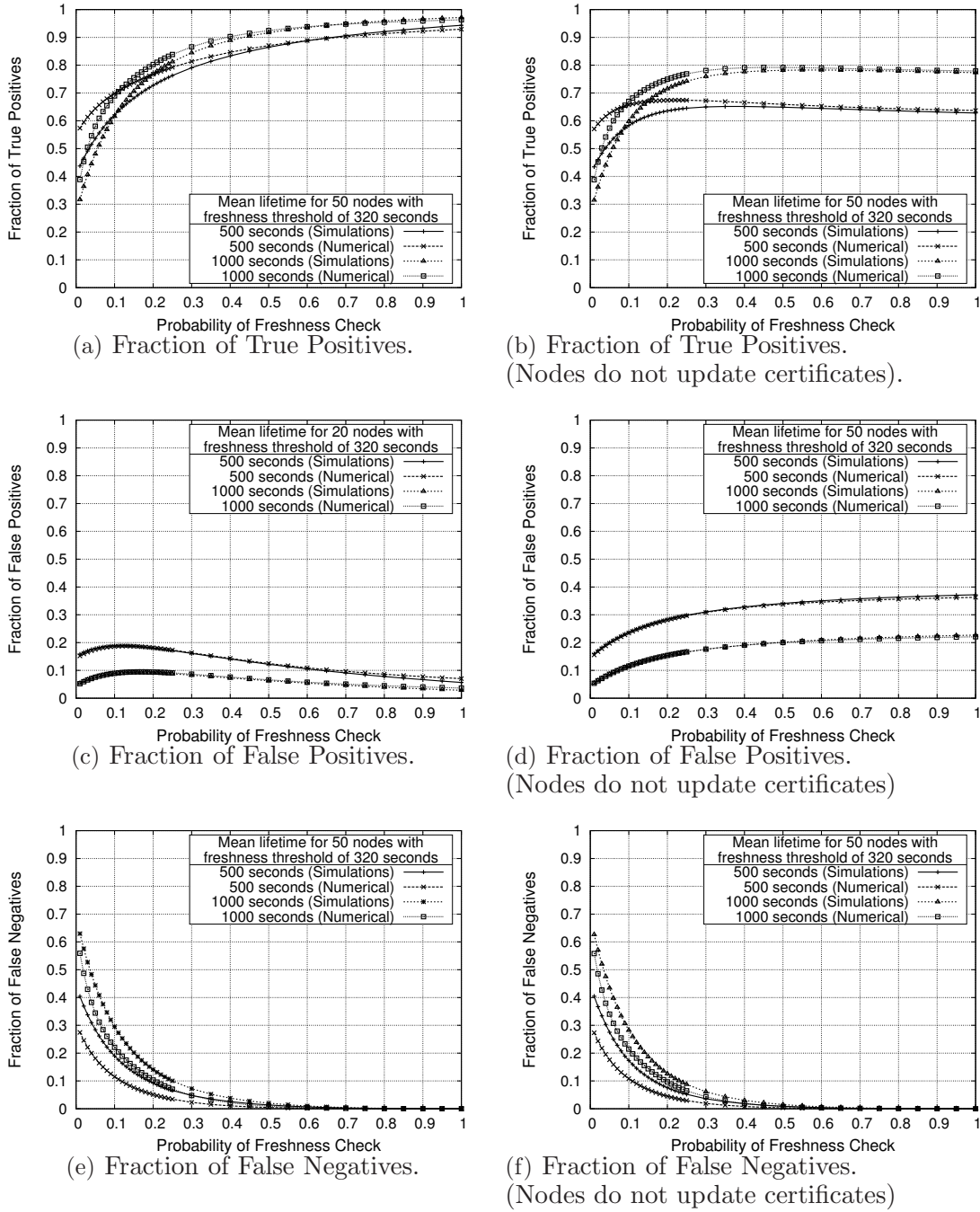
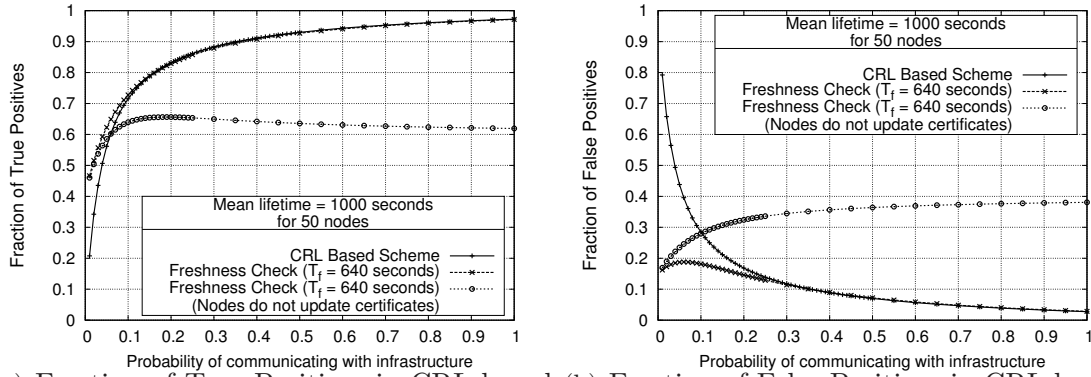


Figure 3.14: Impact of revocation rate in Freshness Check Scheme when revocation occurs due to faults.

hence the total number of False Positives are independent of the device lifetime (and hence revocation rate) however as the total number of True Positives decreases as



(a) Fraction of True Positives in CRL based schemes and Freshness Check scheme. (b) Fraction of False Positives in CRL based schemes and Freshness Check scheme.

Figure 3.15: Comparison of Fraction of True Positives and False Positives in CRL based schemes and Freshness Check scheme

the lifetime decreases, the fraction of False Positives, as shown in Figure 3.14(c) and Figure 3.14(d), increase as the lifetime decreases.

A comparison of the fraction of True Positives and fraction of False Positives in the CRL based scheme and the Freshness Check scheme when $T_f = 160$ seconds is shown in Figure 3.15. The Freshness Check based schemes is able to give a security performance comparable to the CRL based scheme only when the nodes update their certificates on Freshness Checks performed after revocation, while the performance is severely degraded if the nodes do not update their certificates. The higher fraction of True Positives observed in Figure 3.15(a) for the Freshness Check scheme for small values of P_f ($P_f < 0.1$) is because the Freshness Threshold T_f controls the number of False Positives as shown in Figure 3.15(a). These observations can be interpreted in the following ways:

1. As the Freshness Check scheme introduces False Negatives, CoS is not a good metric to compare it with the CRL based schemes, and hence we resort to Fraction of True Positives to compare these schemes.
2. Freshness Check schemes can perform better when the T_f values are selected to keep the False Positives and False Negatives under control.
3. The Freshness Check scheme can provide a higher fraction of True Positives compared to the CRL based scheme when the infrastructure presence is low and

misbehavior is only due to faults. Thus, making them suitable for applications that are capable of tolerating a low fraction of True Positives and regions of low infrastructure presence.

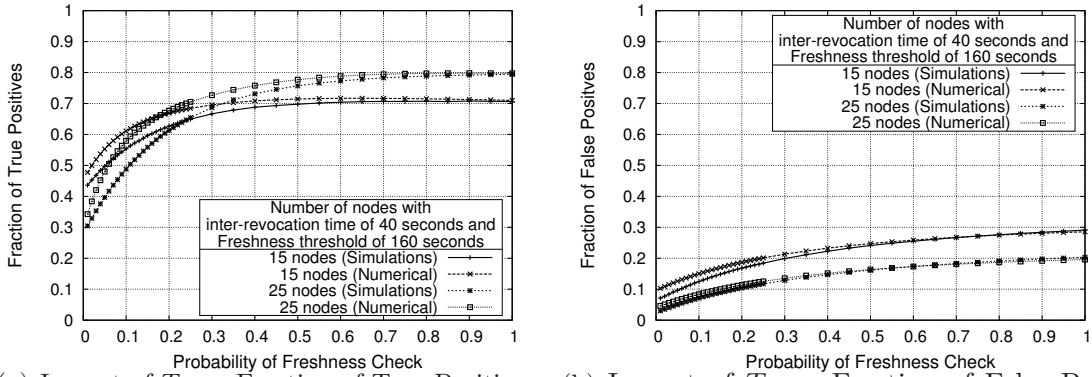
4. The certificates should be installed in the OBU after *each* Freshness Check operation to ensure that the performance of the system does not degrade.

3.5.2.2 Misbehavior due to Maliciousness

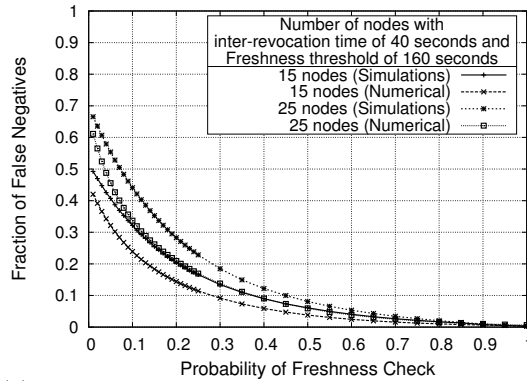
We now study misbehavior due to intentional malicious behavior exhibited by the nodes. We assume that the malicious nodes do not update their certificates when the Freshness Check of their certificates fail. The total time in which packets from a legitimate node are accepted increases with node density which can be obtained from Equation 3.11. This affects the False Negatives as the total time for which the $M/D/\infty$ remains idle is a monotonically increasing function. Thus the False Negatives increase with the node density as shown in Figure 3.16(c). However this increase is not linear as shown in Figure 3.11. Further, the total number of False Positives is independent of node density, hence, as total number of packets from legitimate nodes increase with node density, the fraction of False Positives decrease with node density as shown in Figure 3.16(b). Thus, the fraction of True Positives increase with node density for a given revocation rate and Freshness Check Threshold, as shown in Figure 3.16(a).

As shown in Figure 3.17(a), when the time between successive revocations increase from 20 seconds to 40 seconds, the total time from which packets from legitimate nodes are accepted increases, thus reducing the Fraction of False Positives which depends only on the Freshness Check Threshold. Increasing the Freshness Check Threshold increases the window of vulnerability, hence, when we increase the Freshness Check Threshold from 160 seconds to 320 seconds we observe an increase in the fraction of False Positives in Figure 3.17(b).

The total time for which the $M/D/\infty$ remains idle is a monotonically increasing function, hence, in Figure 3.18(a) we observe an increase in the fraction of False Negatives when the time between successive revocations is increased from 20 seconds

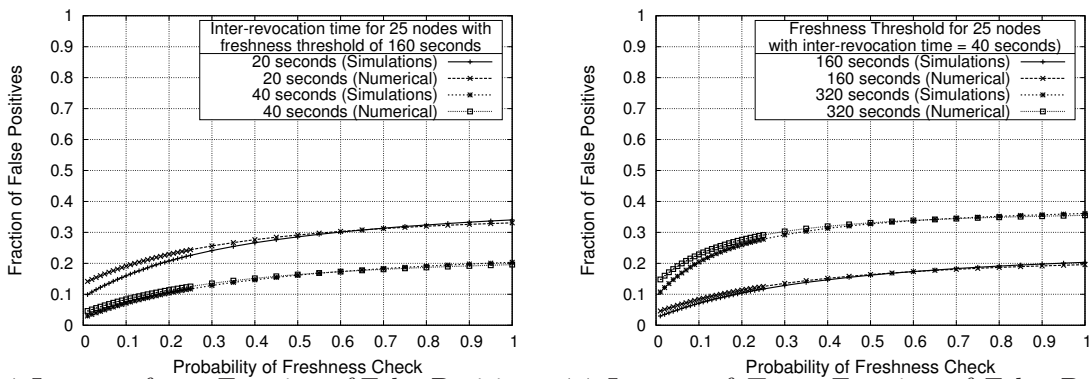


(a) Impact of T_f on Fraction of True Positives. (b) Impact of T_f on Fraction of False Positives.



(c) Impact of T_f on Fraction of False Negatives.

Figure 3.16: Impact of node density in Freshness Check Scheme when revocation occurs due to intentional misbehavior.



(a) Impact of r on Fraction of False Positives. (b) Impact of T_f on Fraction of False Positives.

Figure 3.17: Impact of revocation rate and Freshness Threshold on fraction of False Positives when revocation occurs due to intentional misbehavior.

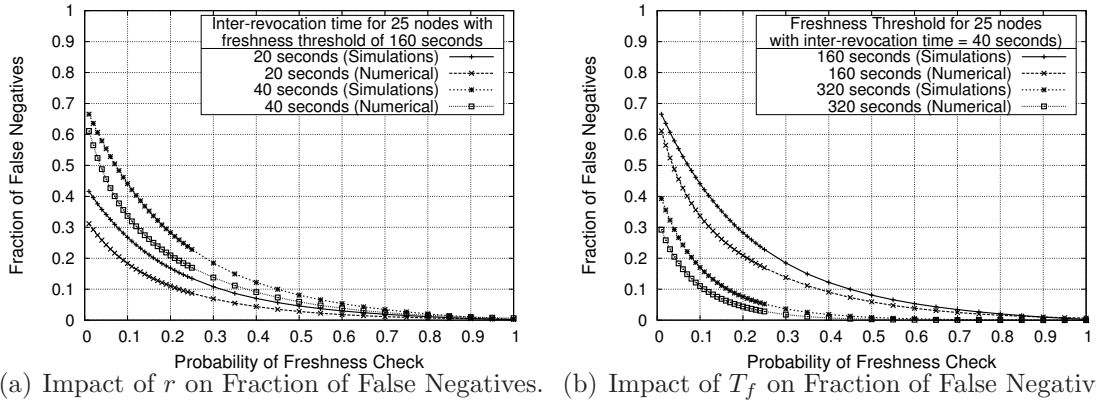


Figure 3.18: Impact of revocation rate and Freshness Threshold on fraction of False Negatives when revocation occurs due to intentional misbehavior.

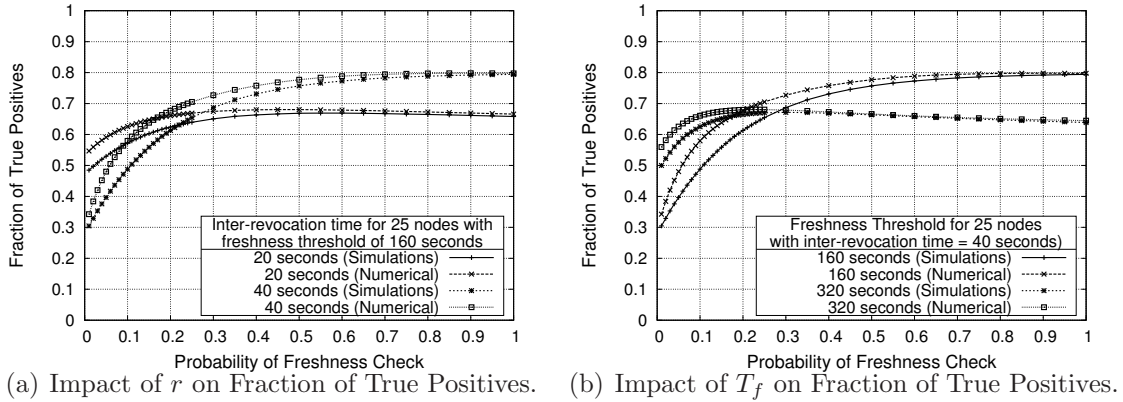


Figure 3.19: Impact of revocation rate and Freshness Threshold on fraction of True Positives when revocation occurs due to intentional misbehavior.

to 40 seconds. An increase in the Freshness Check Threshold increases the busy periods of the $M/D/\infty$ queue, hence, we observe a decrease in the fraction of False Negatives in Figure 3.18(b) when we increase the Freshness Check Threshold from 160 seconds to 320 seconds.

According to Equation 3.11, the total number of True Positives increases as the revocation rate (inverse of the time between successive revocations) decreases, hence, Figure 3.19(a) shows that the fraction of True Positives increases as the time between successive revocations increases from 20 seconds to 40 seconds.

3.6 Summary

In this chapter we highlighted the dilemma at each receiver while accepting a packet signed using a certificate whose revocation information is not present in the CRLs at the OBU. We then proposed a metric, Confidence on Security Infrastructure (CoS), to evaluate the performance of the accept/drop mechanism used at the security layer in the CRL based schemes. We proposed the Freshness Check scheme to address the problem of dissemination of revocation information. We modeled the misbehavior due to faults developed in the devices used to generate and exchange messages in vehicular networks, and due to intentional malicious activities to study the security performance of the CRL based scheme and the Freshness Check scheme. Our analysis shows that the security performance of both the schemes is independent of the node density when misbehavior is only due to faults. Thus, the minimum infrastructure presence required for a desired security performance is independent of the node density, and the rate at which new V2V enabled nodes arrive in the system. The CoS cannot be used to compare the CRL based schemes and the Freshness Check scheme due to the existence of False Negatives in the Freshness Check scheme, hence one must resort to other metrics like fraction of True Positives used in our analysis. The performance of the Freshness Check scheme degrades considerably if the freshness information of the certificates are not updated by the OBU after revocation. We also show that Freshness Check Scheme can perform better than the CRL based schemes in regions where the rate of communication with the infrastructure is low, or the costs of communicating with the infrastructure are high.

Chapter 4

Performance of Communication in Vehicular Networks

We shall now study the communication performance of secure communication in vehicular networks. An overview of the overheads of PKI based security, the proposed security mechanism for safety applications in vehicular networks, is provided in Section 4.1. We then study the performance of V2V communication considering the impact of the computational overheads of security in Section 4.2. As the messages exchanged in vehicular networks rely heavily on the broadcast services of the lower layers of the protocol stack, we study the performance of the broadcast communication in Section 4.3.

4.1 Overheads of Security

The overheads due to security provided by the Public Key Infrastructure (PKI) can be broadly categorized as *computational overheads* and *bandwidth overheads*. The computational overheads arise because the security-related operations such as signing and verifying, require a finite amount of time for completion at the processor of each principal in vehicular networks, while the bandwidth overheads arise due to the headers and footers associated with the security mechanism resulting in extra over-the-air bytes, and control information exchange such as dissemination of revocation information over the communication medium.

The activities that result in the computational overheads include:

1. **Certificate Selection:** Before signing a message a certificate needs to be selected from a pool of valid certificates for ensuring anonymity [47; 53; 57].

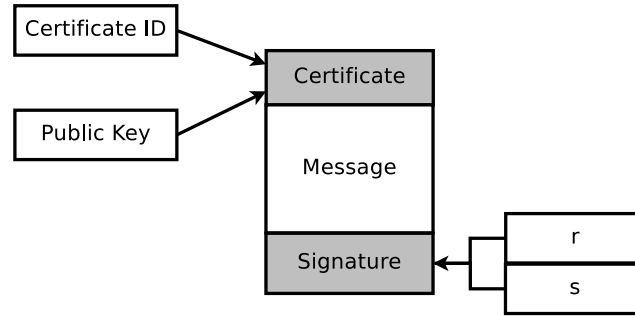
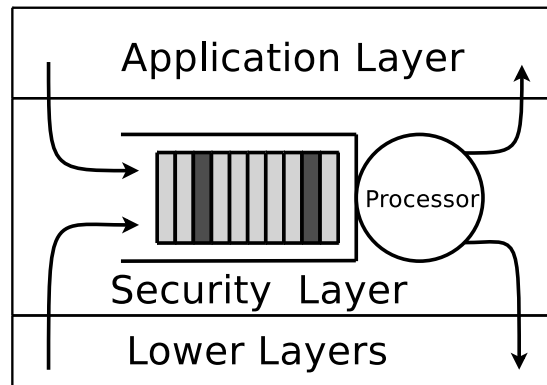


Figure 4.1: Overheads of Security

2. **Signing Messages:** On receiving a message to be secured, the hash of the message is computed which is then signed (encrypted) using the private key corresponding to the certificate selected. This signature and the certificate is then sent to the lower layers along with the message for transmission. In the case of Elliptic Curve Digital Signature Algorithm (ECDSA), the proposed algorithm for securing vehicular networks [9], the signature has two components, r and s ; the signature is computed again if one of the signature components r or s turns out to be 0 [35].
3. **Verifying Certificate:** On receiving a message, the certificate is considered valid if it is not available in the Certificate Revocation Lists (CRLs) present in the On Board Unit (OBU) in case of the CRL based schemes, or the certificate is considered *fresh* in case of the Freshness Check Scheme.
4. **Verifying Message:** In the case of ECDSA, the hash of the message is computed and used with the signature component s to obtain r . This value of r is compared with the one present in the signature.

The bandwidth overheads include:

1. **Increased Message Size:** As shown in Figure 4.1, the packet transmitted over the air contains the message to be exchanged along with the certificate used to sign the message and the signature.
2. **Dissemination of Revocation Information:** In the CRL based schemes, the CRLs need to be disseminated from the infrastructure to each principal in the network that can potentially receive messages signed using the certificates





-  Packet from the neighbors
-  Packet generated by the application layer

Figure 4.2: Queueing at the Security Layer

present in the CRLs. In the case of Freshness Check scheme, the nodes have to periodically perform Freshness Check operations to ensure that their certificates are *fresh*.

4.2 Impact of Computational Overheads

The prior works related performance modeling of vehicular networks do not consider the computational overheads of security as packet transmission and not packet processing is traditionally considered to be the bottle-neck. This results in the question, “Does V2V communication with security scale?”, being unanswered. To study the communication performance of vehicle-to-vehicle (V2V) communication with security we study the communication performance of the Cooperative Collision Warning (CCW) application. CCW is one of the proposed safety applications to actively monitor the kinematics status of the neighboring vehicles to avoid potential collision. This is achieved by secure exchange of periodic messages that contain the kinematics information of the vehicles [63]. This application was selected for performance evaluations due to its periodic message generation, as the system load of the periodic messages is considerably more than the sporadic messages generated by some of the proposed

event based applications. The CCW messages undergo cryptographic operations at the source and the destination. This results in packets generated by the application running on an OBU contending for the services of the processor of the OBU along with the packets arriving from the neighboring vehicles. Simultaneous arrival of CCW messages at the security layer results in queuing of packets, as show in Figure 4.2. The delays due to the time spent at the queue in the security layer can result in packets being dropped due to the stringent latency requirements. We currently assume that all packets (packets received from the neighbors and those generated by the application layer) have the same priority and do not consider priority queues at the security layer.

4.2.1 Queuing at Security Layer

A simple analysis of the queuing system is given as follows. We assume a *single cell* of n_v nodes exchanging messages generated by the CCW application. *To study the impact of the computational overheads on the maximum number of nodes that can be supported in a single cell for the security queue to be stable, we model the computational overheads as the delays involved in the cryptographic operations at the security layer* . Each of these n_v vehicles generates a new message once every t_p seconds. At each node, packets from the application layer arrive at the security layer at a rate of $\frac{1}{t_p}$ (messages/second). We assume that the time spent at the MAC layer (t_m) by each packet is negligible, i.e, $t_m \ll t_p$. The security layer at each node *can receive* $\frac{(n_v - 1)}{t_p}$ messages from the $n_v - 1$ neighbors, thus the maximum arrival rate at the queue in the security layer is $\frac{n_v}{t_p}$. Assuming the processing time of each of the packets at the security server of source and destination is t_s seconds ($t_s < t_p$), the service rate of the queue at the security server is $\frac{1}{t_s}$. Thus, the stability criterion of the queue at the security layer considering only messages related to CCW is $\frac{n_v}{t_p} < \frac{1}{t_s}$. Hence, the maximum number of nodes in a cell for the security queue to be stable is

$$n_v < \frac{t_p}{t_s}. \quad (4.1)$$

The number of vehicles is related to the transmission range and the vehicle density. This relation is obtained as follows. Consider a marked vehicle V_m traveling in a l lane road. Vehicles in lane i travel with a velocity of v_i meters/second. The center of lane i is at a distance d_i meters from the center of the lane in which V_m is traveling. A safety distance of s_{di} seconds of travel is maintained between any 2 vehicles in lane i . Based on these parameters the number of vehicles n_v is given by

$$n_v = \sum_{i=1}^l n_{vi} = \sum_{i=1}^l \frac{2\sqrt{t_r^2 - d_i^2}}{v_i s_{di}} \quad (4.2)$$

Hence for the stability of system

$$\frac{1}{t_p} * \sum_{i=1}^l \frac{2 \cdot \sqrt{t_r^2 - d_i^2}}{v_i \cdot s_{di}} < \frac{1}{t_s} \quad (4.3)$$

Assuming that $t_r \gg d_i$ for all i , and all the vehicle travel with a velocity v_{sd} maintaining a safety distance of s_d seconds of travel. The density of vehicles ρ can be given as $\rho = \frac{l}{v \cdot s_d}$. Hence the number of vehicles n_v is $n_v = 2 \cdot t_r \cdot \rho$. Equation 4.3 can now be written as

$$\frac{2 \cdot t_r \cdot \rho}{t_p} < \frac{1}{t_s} \quad (4.4)$$

Henceforth, we abstract the vehicle density and transmission range using the number of vehicles in the single cell (n_v).

CCW relies on the broadcast services of the Medium Access and Control (MAC) layer of the protocol stack. Broadcast packets in the IEEE 802.11 wireless networks undergoing collisions are not retransmitted as the recipients do not acknowledge individual broadcast packets and the source of the transmission cannot detect collisions [13]. Thus, when P_c denotes the steady state probability of packet collisions, the packets from the $n_v - 1$ neighboring nodes arrive at the security layer with a probability $\frac{P_c(n_v - 1)}{t_p}$. The scalability criterion considering the impact of packet collisions can be given as

$$\frac{P_c(n_v - 1) + 1}{t_p} < \frac{1}{t_s}. \quad (4.5)$$

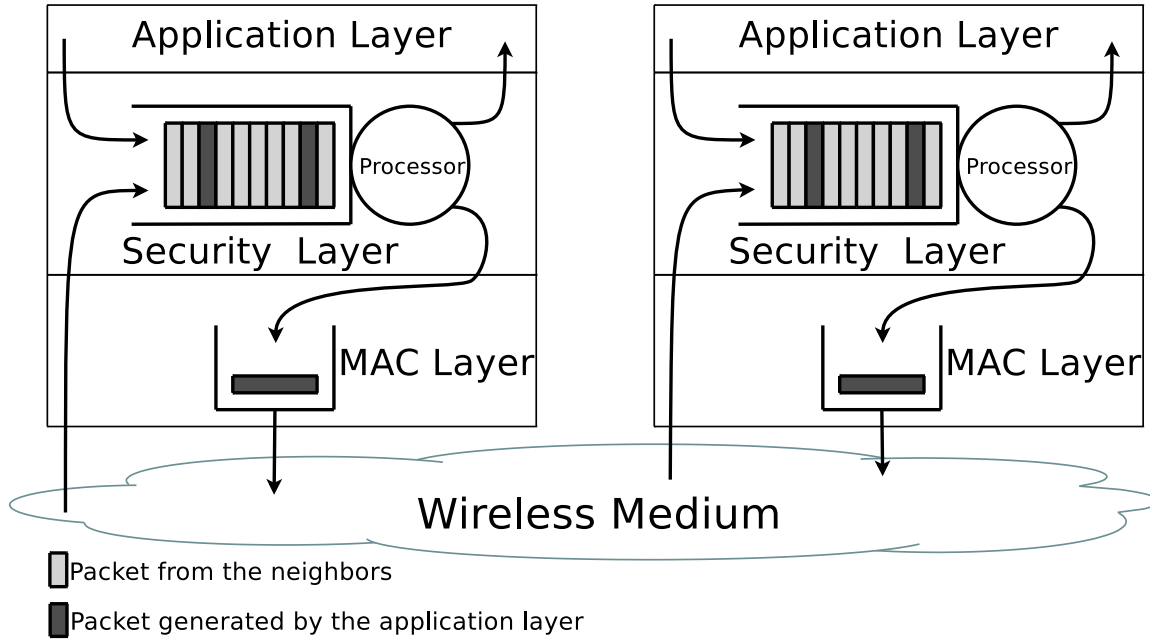


Figure 4.3: Queuing at the Security Layer and the MAC Layer

4.2.2 Simulation Framework to Study Queuing System

We now study the queuing system given in Figure 4.3 using Simulations performed using the *ns2* [3] network simulator. For abstracting the MAC layer, the standard 802.11 implementation available in *ns2* was used. A new application layer (agent) for generating periodic messages and accepting messages from other nodes was added to the *ns2* the details of which are provided in Section A.1. This layer generates packets once every t_p seconds, where t_p is the message generation interval of CCW messages. Each packet spends t_{ss} seconds at the security server of source and t_{sd} seconds at the security server of the destination. Packets arriving at the security layer when a cryptographic operation is being performed are added to the queue in the security layer.

The assumptions made for the simulations are as follows:

1. *Single Cell*: All nodes present in the system are part of a single wireless cell. The channel model used in this cell is the free space model. Under this assumption, each node present in the system is able to hear every other node, hence, packets

undergoing collision are lost from the system and are not received by *any* node. This results in a uniform impact of the wireless medium on all the nodes present in the system.

2. *Deterministic Packet Arrivals*: The packets are generated by the application layer once every t_p seconds with a small jitter of up to 1 ms. The time of generation of the first packet is a uniformly selected from the interval $(0, t_p)$. Each of the packets have a fixed expiry time t_{exp} .
3. *Uniform Cryptographic Delays*: The time spent at the cryptographic server at the source (t_{ss}) and destination (t_{sd}) are the same, i.e., $t_{ss} = t_{sd} = t_s$. Ideally the verification time for ECDSA and other signing algorithms is more than the signing time [53].
4. *Unbounded Buffer*: The buffers at the security queue and the MAC queue are infinite.
5. *FIFO Queuing*: The queuing policy at the security layer and the MAC layer is FIFO as shown in Figure 4.3.
6. *Malicious Nodes*: None of the nodes present in the cell are malicious. We currently do not study the impact of malicious activities on the communication performance of vehicular networks.
7. *Fixed Packet Sizes*: The data is exchanged in packets of 250 bytes [9].
8. *MAC Layer*: 802.11a was used as the MAC layer with a data rate of 6 Mbps.

4.2.3 Numerical Results and Discussions

The following values were used for simulating the impacts of computational overheads on the number of nodes that can exchange secure CCW messages.

t_p The message generation rate was kept fixed at 100 milliseconds [63].

t_{exp} The message expiry time was varied from 50 milliseconds to 300 milliseconds.

We also study the system when the expiry time is infinite.

t_{ss} The time spent for cryptographic operations were varied from 5 milliseconds to 15 milliseconds [53]. In the plots, $t_s = x$ milliseconds implies that t_s was uniformly selected from the interval $(x, x+1)$ milliseconds. The reason for the randomness

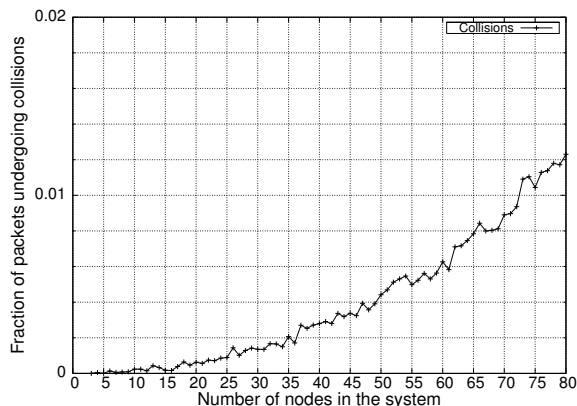


Figure 4.4: Packets lost to collisions when there are no delays at security layer.

in time required for signing and verifying packets is as follows. Generating the signature component using the ECDSA algorithm may require computation of the signature components r and s more than once resulting in the variance of cryptographic delays at the source. Further, searching the certificate in the CRLs and validating the certificate may result in variance of cryptographic delays at the destination.

n_v The number of nodes exchanging messages was varied from 3 to 100.

Each point shown in the plots is an average of 25 randomly seeded simulation runs.

When there are no computational overheads of security (or when the messages are not secured) and the packet expiry time is infinite then packets are lost only to collisions at the MAC layer. Hence, if P_{cn} is the steady state probability of collision when there are n_v nodes present in the single cell, then the probability that a packet generated by a node is received by all the $n_v - 1$ other nodes in the cell is $1 - P_{cn}$. When there are no cryptographic delays at the security layer ($t_s = 0$), and packets are generated once every 100 milliseconds with an infinite expiry time ($t_{exp} = \infty$), then Figure 4.4 shows that increasing the node density increases the fraction of packets undergoing collisions. Further, we observe that the system is capable of supporting more than 80 nodes as only 1% of the packets are lost, i.e, 99% of the packets generated are received by all the neighbors of the source of the packet.

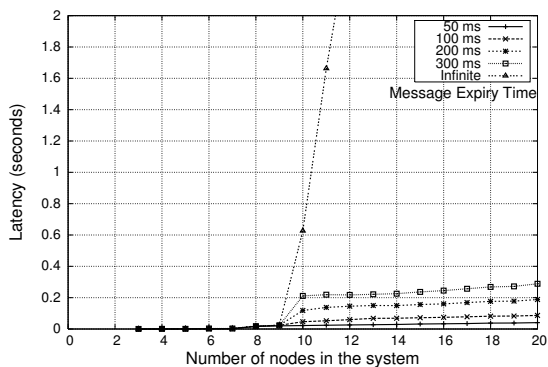


Figure 4.5: Time spent at the security queue of the source of the packet.

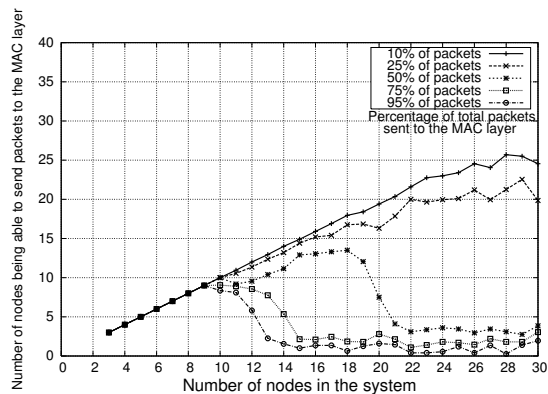
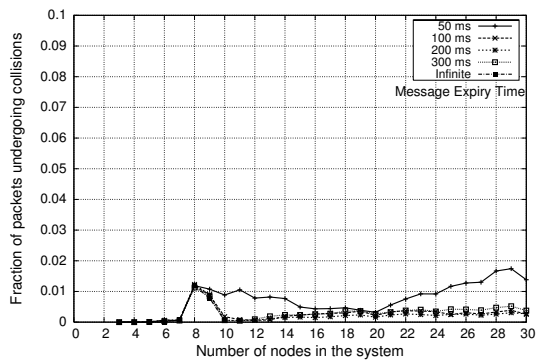
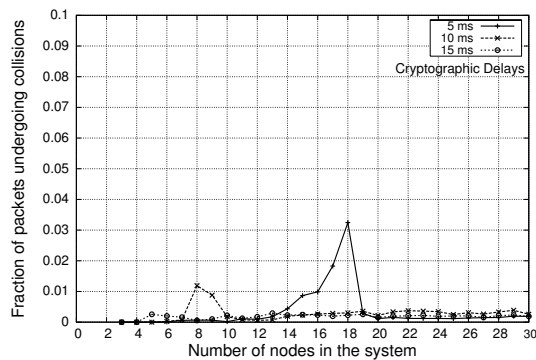


Figure 4.6: Number of nodes successful in sending packets to the MAC layer.



(a) Fraction of packets that are lost to collisions for different packet expiry times.



(b) Fraction of packets lost to collisions for different different signing delay.

Figure 4.7: Packets lost to collisions when there are delays at security layer

When the computational overheads result in a cryptographic operations taking 10.5 (t_s randomly selected from the interval (10, 11)) milliseconds for each packet at the source and destination, then the time spent at the security queue of the source of the packet is given in Figure 4.5. We observe that the security queue is unstable for $t_{exp} = \infty$ when $n_v > \frac{t_p}{t_s}$. When the packets have a finite expiry time, then packets that have not expired or shall not expire during the processing of the packet are processed by the server serving the security queue; the rest of the packets are dropped. Thus, only a fraction of total packets generated by the application layer are sent to the MAC layer. Figure 4.6 shows the number of nodes that are able to send at least a given fraction of packets to the MAC layer when the expiry time is set to

100 milliseconds. We observe that for $n_v < \frac{t_p}{t_s}$, all the nodes are able to send at least 95% of the packets to the MAC layer, however when $n_v > \frac{t_p}{t_s}$ we observe that only a small number of nodes are able to send at least 75% packets to the MAC layer.

Further, the packets arriving at the MAC layer are lost due to collisions as shown in Figure 4.7. Figure 4.7(a) shows the fraction of packets lost to collisions when the computational delays due to the cryptographic operations was randomly sampled from the interval (10,11) milliseconds. As the simulations were stopped after 100 seconds (generation of approximately 10000 packets by each node), and due to the delays at the security layer, most of the packets generated were queued up at the security layer when the expiry time was infinite and $n_v > \frac{100}{10.5}$. As the queues were unstable when $n_n > \frac{100}{10.5}$ and the simulations were conducted only a finite amount of time we obtain only a small fraction of packets lost due to collisions when the expiry time was set to infinite in Figure 4.7(a).

This preliminary study of the impact of computational overheads was extended by Iyer *et al.* [34]. When the packets are generated by the application layer according to a Poisson process with a mean inter-arrival time of t_p seconds and the computational delays are exponentially distributed with a mean t_s , then the end to end throughput of packets from any given node to any other node is given by (according to [34, Equation 6])

$$\lambda_{e2e} = \frac{(1 - P_b)^2(1 - P_c)}{t_p}$$

where P_b is the blocking probability of the packet at the security layer and P_c is the steady state probability of packet collision.

Many safety applications like CCW use the broadcast services of the MAC layer for exchanging safety messages in vehicular networks. The packets undergoing collisions in broadcast networks based on the IEEE 1609.4 standard (which is based on the IEEE 802.11 standard) are not retransmitted by the MAC layer as the source is not able to detect collisions and the recipients do not acknowledge the broadcast packets. In the next section we study the performance of such broadcast networks where the MAC layer does not retransmit packets that are lost due to collisions.

4.3 Performance of Broadcast Communication

In this section we present the performance of broadcast communication used in vehicular networks. Specifically, we consider an IEEE 802.11 wireless ad hoc network where applications like CCW communicate with each other using the broadcast services of the MAC layer. Clearly, in a broadcast environment where there exists no direct mechanism to infer the loss of information owing to collisions in the transmission medium, it is important to indirectly and accurately determine the probability of packet collisions. We now propose an analytic model for IEEE 802.11 broadcast-based ad hoc networks. Specifically, a simple finite-state Markov chain model is developed to model the buffer occupancy process for the IEEE 802.11 MAC considering broadcast traffic within a single cell. The steady state transition probabilities are computed as a function of the packet arrival rate at the MAC layer, the probability of transmission, the number of nodes in the cell and the packet length to obtain the probability of collisions and study the stability of the system.

4.3.1 System Model: Assumptions and Notations

We consider a single cell of n homogeneous nodes that communicate with each other using the broadcast services of IEEE 802.11 MAC layer. In IEEE 802.11 networks, the time is assumed to be slotted and we assume data payloads exchanged of the same size are broadcast with the same data rate resulting in L' busy slots ($L' \geq 1$). If the DIFS occupies d' slots then, on sensing a transmission, the other nodes that have a packet to transmit restart their backoff process after $L = L' + d'$ slots. The wireless channel is assumed to be noiseless i.e., the errors in packet reception due to fading and other external interferences are not considered and we assume losses only due to packet collisions. The packet arrivals from the higher layer are assumed to be based on a Poisson distribution. The system being slotted, these packets arrive with a probability λ in each slot. In the analysis we initially assume λ to be very small ($\lambda \ll 1$), such that all the nodes have at most one packet ready for transmission in any given slot resulting in *bufferless* MAC queues. We later extend this model

to higher packet generation rates to model finite buffers at the MAC layer. All the nodes in the network use the same backoff parameters and *independently* attempt to transmit with a probability β in each slot. The summary of the assumptions made are as follows:

1. There are n homogeneous nodes placed in a single cell wireless topology, i.e., the n nodes are able to hear each other. The number of nodes present in the single cell (n) can be used to abstract the node density and transmission range of the devices used.
2. The data exchanged is of a fixed size resulting in busy periods of a fixed number of slots (L). The length of the busy period (L) is the effective time the bytes of the packet are transmitted over the air which can be used to abstract the packet length and the data transmission rates.
3. The nodes that have a packet attempt a transmission with a probability β in each slot when the channel is idle, i.e., the backoff counter for packet transmission is sampled from a geometric distribution. This abstracts the contention window of IEEE 802.11.
4. The arrival rate λ that abstracts the packet generation process at the application layer is based on a Poisson distribution.

4.3.2 Modeling Bufferless MAC

The wireless channel is seen by all the nodes to be either busy or idle as shown in Figure 4.8. When the arrival rates are low ($\lambda \ll 1$), at the end of a busy period, the nodes can either have a backlogged packet ready for transmission or be awaiting an arrival of a packet from the higher layer. Each node at the end of the busy periods can be *independently* modeled using a two-state Markov Chain as shown in Figure 4.9. State 0 represents the state where the node does not have any packets at the MAC queue while State 1 represents the state where the node has exactly one packet and is performing the backoff process.

We assume that at the end of each busy period, the state of each node (either 0 or 1) is *independent* of the state of other nodes present in the system. Let P_{10} denote

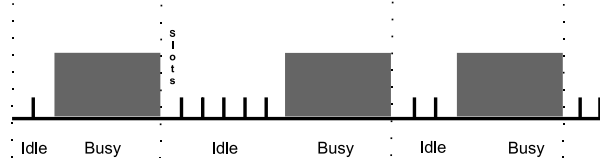


Figure 4.8: Broadcast of fixed size packets

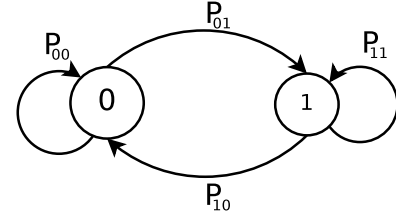


Figure 4.9: Two State Markov chain for a node

the steady state transition probabilities from State 1 to State 0 and $P_{10}(k)$ denote the probability of a transition from State 1 to State 0 by a node in a cycle, when there are k other nodes ($0 \leq k \leq n - 1$) contending for the channel.

The value of $P_{10}(k)$ is derived as follows. Consider a marked node that has a packet to transmit at the end of a busy cycle. In the first slot just after a busy period if k nodes other than the marked node have a packet to transmit then, based on the bufferless assumption, there can be j nodes ($0 \leq j \leq n - k - 1$) that can receive a packet from the higher layer. The transmit probability β is assumed to independent of the state of each of the other $n - 1$ nodes in the system, hence, if this node and the k other nodes having a packet do not transmit, then the next slot can be visualized as the first slot after a busy period in which $k + j$ nodes have a packet to transmit. $P_{10}(k)$ can be given as

$$P_{10}(k) = \sum_{j=0}^{n-k-1} \binom{n-k-1}{j} \lambda^j (1 - \lambda)^{n-k-1-j} (1 - \beta)^{k+1} P_{10}(k + j) + \beta. \quad (4.6)$$

Similarly, let P_{01} denote the steady state transition probability that a node at State 0 at the beginning of the cycle ends up in State 1 at the beginning of the next cycle and $P_{01}(k)$ denote the probability of that a node undergoes a transition from State 0 to State 1 when there are k nodes ($0 \leq k \leq n - 1$) contending for the channel. As in the case of $P_{10}(k)$, we consider a marked node that is in State 0 at the end of the busy period. In the first slot after a busy period, there can be j nodes that receive a packet from the higher layer ($0 \leq j \leq n - k - 1$). If none of the k nodes attempt a transmission, the arrival process being geometric, the next slot can be modeled as

the first slot after a busy period in which there are $k + j$ nodes that have a packet to transmit. If there were no arrivals at the marked node then the next slot can be modeled as $P_{01}(k + j)$ and if there was an arrival at the marked node then the next slot can be modeled as $P_{11}(k + j)$. $P_{11}(k)$ the transition probability of being in State 1 at the end of a busy period if the node was in State 1 at the beginning of the cycle when k other nodes had a packet to transmit, i.e., $P_{11}(k) = 1 - P_{10}(k)$. Further, if there is a transmission attempt before there is an arrival at the marked node, then the node undergoes a transition from State 0 to State 1 if there was an arrival in the L slots in which the system was busy. Hence, $P_{01}(k)$ can be given as

$$\begin{aligned}
P_{01}(k) = & \left(1 - (1 - \beta)^k\right) \left(1 - (1 - \lambda)^{L+1}\right) + \\
& \sum_{j=0}^{n-k-1} \binom{n-k-1}{j} \lambda^j (1 - \lambda)^{(n-k-1-j)} (1 - \beta)^k \\
& ((1 - \lambda) P_{01}(k + j) + \lambda P_{11}(k + j)). \tag{4.7}
\end{aligned}$$

Let π denote the steady state probability that a node has a packet at the beginning of the cycle. As the nodes are assumed to be homogeneous, the steady state value for π at each node will be the same. The steady state values of P_{01} and P_{10} can be computed from $P_{01}(k)$ and $P_{10}(k)$ for a given value of π as follows.

$$P_{01} = \sum_{k=0}^{n-1} \binom{n-1}{k} \pi^k (1 - \pi)^{n-1-k} P_{01}(k) \tag{4.8}$$

$$P_{10} = \sum_{k=0}^{n-1} \binom{n-1}{k} \pi^k (1 - \pi)^{n-1-k} P_{10}(k) \tag{4.9}$$

The value of $P_{10}(n - 1)$, numerically computed from Equation 4.6, can be used to compute $P_{10}(k)$ for $n - 1 > k \geq 0$ that can be substituted in Equation 4.9 to give P_{10} . Similarly P_{01} can be computed using the previously computed values of $P_{10}(k)$ and by computing $P_{01}(k)$ for $n - 1 > k \geq 0$ using the value of $P_{01}(n - 1)$ computed

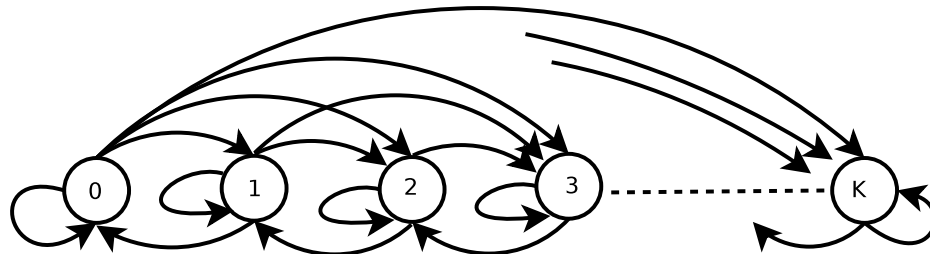


Figure 4.10: Markov Chain for a node with finite buffer

from Equation 4.7. The value of π can be obtained as from P_{01} and P_{10} as

$$\pi = \frac{P_{01}}{P_{01} + P_{10}}. \quad (4.10)$$

Using this value of π , we shall now obtain the probability of packet collisions. At the end of the busy cycle, a node independently attempts a transmission in each slot with a probability $\pi\beta$. The packet transmitted is successfully received by all the other nodes only if *none* of the other nodes attempt a transmission in the same slot. Hence the probability of successful transmission is given by $(1 - \pi\beta)^{n-1}$ and the probability of collisions as the fraction of attempted transmissions undergoing collisions is

$$P_{coll} = 1 - (1 - \pi\beta)^{n-1}. \quad (4.11)$$

4.3.3 Modeling MAC with Finite Buffers

We now relax the constraint of low packet generation rates and assume all possible values for λ , i.e, $0 < \lambda \leq 1$. For this, we assume that each node has a storage capacity of K units. The buffer size K will now serve as another system parameter. One important problem for such systems is to obtain the number of nodes n the system *can support*¹ for a given configuration of β , λ , K , and L .

We now look at the MAC layer with finite buffers where packets are queued up

¹The definition of “can support” qualifier above can be subjective. For example, one may state a value for probability of MAC layer collision and another value of packet blocking probability (the probability with which new arriving packets are lost) and then find maximum value of n that satisfies both these constraints.

according to the drop tail queuing principle. Arrivals when a node has a packet to transmit are queued up provided the queue contains less than K elements ($K \geq 1$). At the end of a busy period, each node can be modeled as a Markov Chain of $K + 1$ states as shown in Figure 4.10. State i represents the state where the node has i ($0 \leq i \leq K$) packets in the MAC queue. Let the steady state probability of finding any node in State i at the end of a busy period be π_i , hence $(1 - \pi_0)$ is the probability that a node has *at least* one packet in its buffers available for transmission. Thus, each node independently attempts a transmission in a slot with a probability $(1 - \pi_0)\beta$ when the channel is sensed idle. Hence, the probability of collisions as the fraction of attempted transmission undergoing collisions for this system can be given as

$$P_{coll} = 1 - (1 - (1 - \pi_0)\beta)^{n-1}. \quad (4.12)$$

The transition probabilities from State i to State j ($P_{i,j}$), where $i, j \in [0, K]$, can be obtained from $P_{i,j}(k)$ indicating the probability of transition from State i to State j when k ($0 \leq k \leq n - 1$) other nodes have a packet to transmit. Thus, from any State i ($0 \leq i \leq K$), a transition to State j ($\max(0, i - 1) \leq j \leq K$) is possible at the end of a busy period with a probability $P_{i,j}(k)$. As there can be *at most* one transmission by a given node in a cycle, the only transitions from State i ($i > 0$) to State j when $j < i$ is when $j = i - 1$. The following equations for $P_{i,j}(k)$ ($i, j \in [0, K]$) will be approximate as we make the assumption that the state of all the nodes in the system are independent of each other at the ends of successive transmissions.

A transition from State 0 to State j ($0 \leq j \leq K - 1$) at a marked node, when k other nodes have a packet to transmit is possible when

1. At least one of the k nodes attempts a transmission and *exactly* j arrivals take place before the start of the next cycle, or
2. Arrivals take place at m ($0 \leq m \leq n - k - 1$) other nodes while none of the k nodes attempt a transmission. In this case, the next slot can be modelled as $P_{0,j}(k + m)$ if there were no arrivals or $P_{1,j}(k + m)$ if there was an arrival at the marked node in the given slot.

Hence, $P_{0,j}(k)$ ($0 \leq j \leq K - 1$) can be given as

$$\begin{aligned}
P_{0,j}(k) &= \left(1 - (1 - \beta)^k\right) \left(\binom{L+1}{j} \lambda^j (1 - \lambda)^{L+1-j}\right) \\
&\quad + \sum_{m=0}^{n-k-1} \binom{n-k-1}{m} \lambda^m (1 - \lambda)^{n-k-1-m} (1 - \beta)^k \\
&\quad \left((1 - \lambda) P_{0,j}(k+m) + \lambda P_{1,j}(k+m)\right). \tag{4.13}
\end{aligned}$$

A transition from State 0 to State K at a marked node, when k nodes have a packet to transmit is possible when

1. At least one of the k nodes attempts a transmission, and *at least* K and *at most* $L + 1$ arrivals take place before the start of the next cycle, or
2. Arrivals take place at m ($0 \leq m \leq n - k - 1$) other nodes while none of the k nodes attempt a transmission. In this case, the next slot can be modelled as $P_{0,K}(k+m)$ if there were no arrivals or $P_{1,K}(k+m)$ if there was an arrival at the marked node in the given slot.

Hence,

$$\begin{aligned}
P_{0,K}(k) &= \left(1 - (1 - \beta)^k\right) \left(\sum_{m=K}^{L+1} \binom{L+1}{m} \lambda^m (1 - \lambda)^{L+1-m}\right) \\
&\quad + \sum_{m=0}^{n-k-1} \binom{n-k-1}{m} \lambda^m (1 - \lambda)^{n-k-1-m} (1 - \beta)^k \\
&\quad \left((1 - \lambda) P_{0,K}(k+m) + \lambda P_{1,K}(k+m)\right). \tag{4.14}
\end{aligned}$$

A transition from State i ($0 < i \leq K - 1$) to State j ($i \leq j \leq K - 1$) at a marked node, when k nodes have a packet to transmit is possible when

1. The marked node does not attempt a transmission while at least one of the k nodes attempts a transmission followed by *exactly* $j - i$ arrivals at the marked node in the $L + 1$ slots available before the next cycle begins, or
2. The marked node attempts a transmission. This is followed by *exactly* $j - i + 1$

arrivals at the marked node in the $L + 1$ slots available before the next cycle begins, or

3. Arrivals take place at m ($0 \leq m \leq n - k - 1$) other nodes and there was no transmission attempt made by the marked node and the k other nodes. In this case, the next slot can be modelled as $P_{i,j}(k + m)$ if there was no arrival at the marked node or $P_{i+1,j}(k + m)$ if there was an arrival at the marked node.

Hence, $P_{i,j}(k)$ ($0 < i \leq K - 1$ and $i \leq j \leq K - 1$) can be given as

$$\begin{aligned}
P_{i,j}(k) &= (1 - \beta) \left(1 - (1 - \beta)^k\right) \left(\binom{L+1}{j-i} \lambda^{j-i} (1 - \lambda)^{L+1-j+i}\right) \\
&\quad + \beta \left(\binom{L+1}{j-i+1} \lambda^{j-i+1} (1 - \lambda)^{L-j+i}\right) \\
&\quad + \sum_{m=0}^{n-k-1} \binom{n-k-1}{m} \lambda^m (1 - \lambda)^{n-k-1-m} (1 - \beta)^{k+1} \\
&\quad \left((1 - \lambda) P_{i,j}(k + m) + \lambda P_{i+1,j}(k + m)\right). \tag{4.15}
\end{aligned}$$

A transition from State i ($0 < i \leq K - 1$) to State K at a marked node, when k nodes have a packet to transmit is possible when

1. The marked node does not attempt a transmission while at least one of the k nodes attempts a transmission followed by *at least* $K - i$ and *at most* $L + 1$ arrivals at the marked node before the next cycle begins, or
2. The marked node attempts a transmission followed by *at least* $K - i + 1$ and *at most* $L + 1$ arrivals at the marked node before the next cycle begins, or
3. Arrivals take place at m ($0 \leq m \leq n - k - 1$) other nodes and there was no transmission attempt made by the marked node and the k other nodes. In this case, the next slot can be modelled as $P_{i,K}(k + m)$ if there was no arrival at the marked node or $P_{i+1,K}(k + m)$ if there was an arrival at the marked node.

Hence, $P_{i,K}(k)$ ($0 < i \leq K - 1$)

$$\begin{aligned}
P_{i,K}(k) &= (1 - \beta) \left(1 - (1 - \beta)^k\right) \left(\sum_{m=K-i}^{L+1} \binom{L+1}{m} \lambda^{m-i} (1 - \lambda)^{L+1-m+i} \right) \\
&\quad + \beta \left(\sum_{m=K-i+1}^{L+1} \binom{L+1}{m} \lambda^{j-i+1} (1 - \lambda)^{L-m+i} \right) \\
&\quad + \sum_{m=0}^{n-k-1} \binom{n-k-1}{m} \lambda^m (1 - \lambda)^{n-k-1-m} (1 - \beta)^{k+1} \\
&\quad ((1 - \lambda) P_{i,K}(k+m) + \lambda P_{i+K,j}(k+m)). \tag{4.16}
\end{aligned}$$

When a node is in State K at the end of a busy period, it remains in State K at the beginning of the next cycle when

1. No transmission attempt made by this node and a transmission attempt was made by *at least* one of the k nodes, or
2. This node attempts a transmission in the first slot of this cycle followed by *at least* one and *at most* $L + 1$ arrivals before the beginning of the next cycle, or
3. Arrivals take place at m ($0 \leq m \leq n - k - 1$) other nodes and there was no transmission attempt made by the marked node and the k other nodes. Thus, the next slot can be modelled as $P_{K,K}(k+m)$.

Hence,

$$\begin{aligned}
P_{K,K}(k) &= (1 - \beta) \left(1 - (1 - \beta)^k\right) + \beta \sum_{m=1}^{L+1} \binom{L+1}{m} \lambda^m (1 - \lambda)^{L+1-m} \\
&\quad + \sum_{m=0}^{n-k-1} \binom{n-k-1}{m} \lambda^m (1 - \lambda)^{n-k-1-m} (1 - \beta)^{k+1} P_{K,K}(k+m). \tag{4.17}
\end{aligned}$$

When a node is in State i ($0 < i \leq K - 1$) at the end of a busy period, it can be found in State $i - 1$ at the beginning of the next cycle when

1. There was a transmission attempt by the marked node followed by no arrivals at the marked node during the busy period, or

2. Arrivals take place at m ($0 \leq m \leq n - k - 1$) other nodes and there was no transmission attempt by the marked node and the k other nodes having at least one packet in their buffers. Thus, the next slot can be modelled as $P_{i,i-1}(k+m)$ only if there were *no arrivals* at the marked node. This is because there can be at most one transmission attempt by any node in a given cycle.

Hence,

$$P_{i,i-1}(k) = \beta(1-\lambda)^{L+1} + \sum_{m=0}^{n-k-1} \binom{n-k-1}{m} \lambda^m (1-\lambda)^{n-k-m-1} (1-\beta)^{k+1} (1-\lambda) P_{i,i-1}(k+m). \quad (4.18)$$

When a node is in State K at the end of a busy period, it can be found in State $K-1$ at the beginning of the next cycle when

1. There was a transmission attempt by the marked node followed by no arrivals at the marked node during the busy period, or
2. Arrivals take place at m ($0 \leq m \leq n - k - 1$) other nodes and there was no transmission attempt by $k+1$ nodes having at least one packet in their buffers. Thus, the next slot can be modelled as $P_{K,K-1}(k+m)$.

Hence,

$$P_{K,K-1}(k) = \beta(1-\lambda)^{L+1} + \sum_{m=0}^{n-k-1} \binom{n-k-1}{m} \lambda^m (1-\lambda)^{n-k-m-1} (1-\beta)^{k+1} P_{K,K-1}(k+m). \quad (4.19)$$

Using the above equations, we can obtain the probability of transition from State i to State j as

$$P_{i,j} = \sum_{k=0}^{n-1} \binom{n-1}{k} (1-\pi_K(0))^k \pi_K(0)^{n-1-k} P_{i,j}(k). \quad (4.20)$$

Parameter	Value
Number of nodes (n)	3 to 200
Probability of transmit in a given slot (β)	1/16 and 1/8
Probability of packet arrival in a given slot (λ)	1/2500 and 1/5000
Number of busy slots (L)	25, 50

Table 4.1: Simulation Parameters

4.3.4 Numerical Results and Discussions

A simple discrete event simulator to simulate the state of the nodes and the wireless channel for 10^6 cycles of busy and idle periods was written based on the algorithm provided in Section A.2. The range of the system parameters used in the simulations were obtained as follows. The slot duration in IEEE 802.11 is $20 \mu\text{s}$ [13] while data rate for vehicular networks is 6 Mbps [63; 25]. Hence, the number of slots L required to transmit a signed message of 250 bytes [9] = $\frac{250 * 8}{6 * 10^6 * 20 * 10^{-6}} \approx 17$. The awareness messages are broadcast once every 100 ms [63; 18], i.e., once every $\frac{100 * 10^{-3}}{20 * 10^{-6}} = 5000$ slots with a transmission range of about 150 meters [63]. Assuming each vehicle of length 4 meters maintains a distance of 2 meters with the vehicle in front of it, we can have $150/6 = 25$ vehicles in each lane giving approximately 150 nodes in a six lane freeway that are in the transmission range of a given node. Using the above information, the simulation parameters given in Table 4.1 were used to study the behavior of the MAC layer when the arrival rates are low.

Figure 4.11 shows the impact of the packet arrival rates on the probability of a node having a packet at the beginning of a cycle (π) and the fraction of packets undergoing collisions (P_{coll}) when $\beta = \frac{1}{16}$ and the time for which the packet is transmitted over the air (L) is 25 slots. We observe that increasing λ from $\frac{1}{5000}$ to $\frac{1}{2500}$ results in an increase in π and P_{coll} as increasing the arrival rates at the MAC layer result in nodes ending up in State 1 in most of the cycles.

Similarly, Figure 4.12 shows the impact of L , the time for which the packet is transmitted over the air, on π and P_{coll} . When $\lambda = \frac{1}{5000}$ and $\beta = \frac{1}{16}$ we observe that

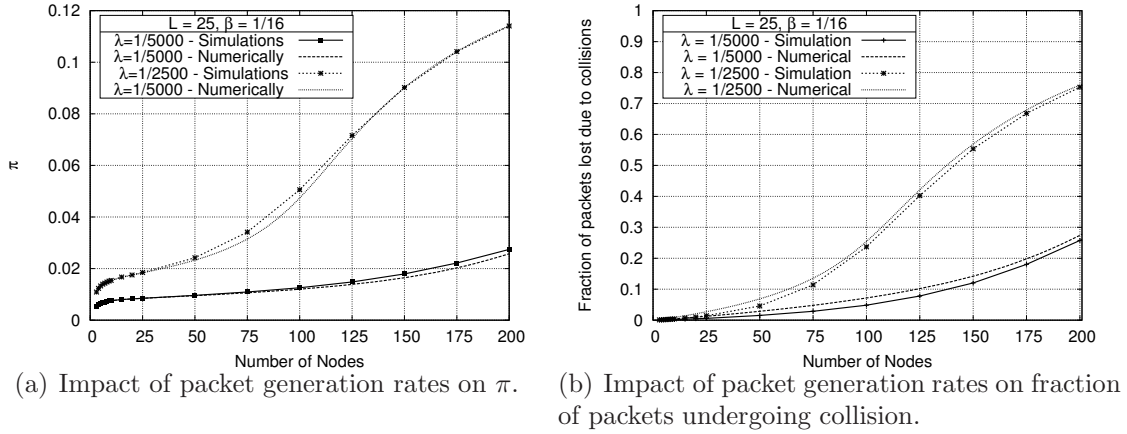


Figure 4.11: Impact of packet generations rates on performance of Bufferless MACs.

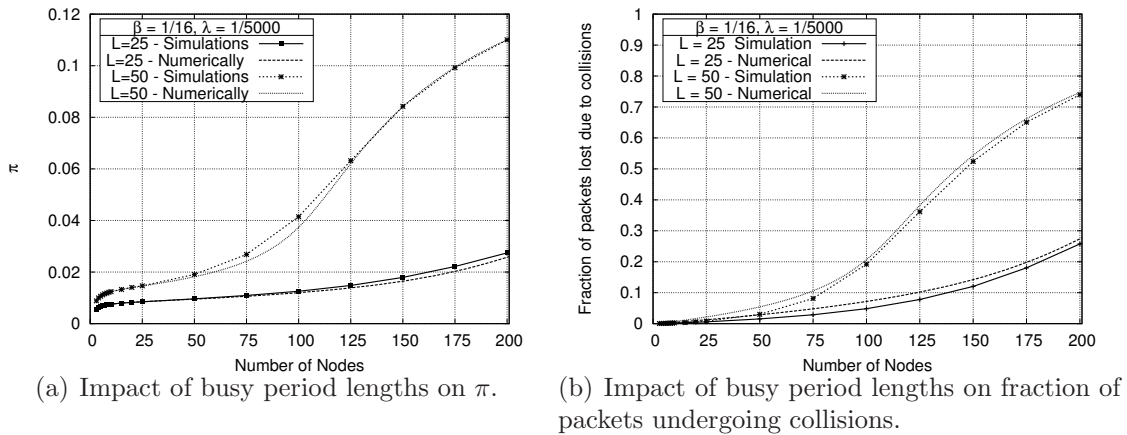
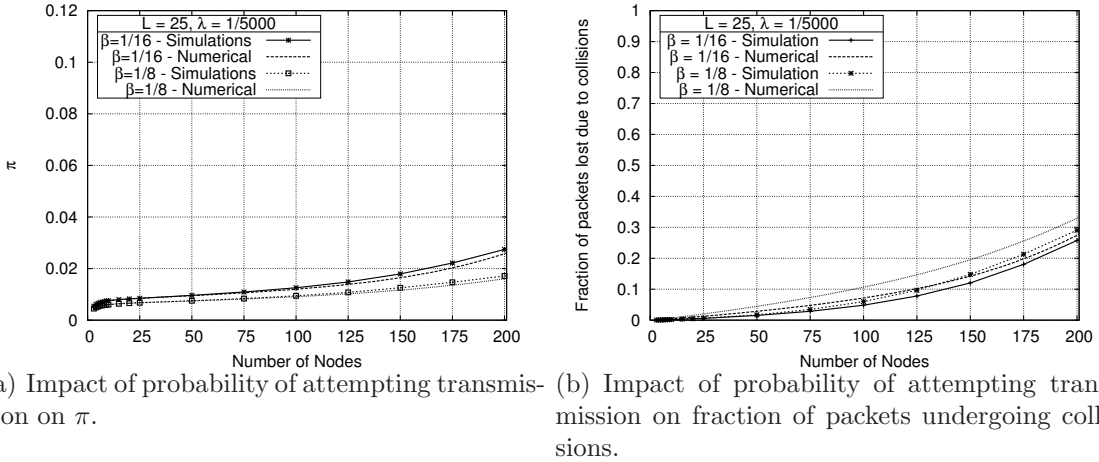


Figure 4.12: Impact of busy period lengths on performance of Bufferless MACs.

decreasing the time for which the packet is transmitted over the air from 50 slots to 25 slots decreases π . This can be explained as follows. Higher values of L indicate an increase in the number of slots for which the channel is kept busy, resulting in increase in the number of slots required to complete a cycle, as shown in Figure 4.8. These extra slots account for the increased number arrivals in the cycle resulting in higher values of π . Hence, for fixed packet sizes increasing the data rate can be used to reduce the values of π and thus packet collisions, as shown in Figure 4.12(b). Further, Figure 4.11 and Figure 4.12 show that increasing the value of λ from $\frac{1}{5000}$ to $\frac{1}{2500}$ has a similar impact to increasing L from 25 slots to 50 slots when $\beta = \frac{1}{16}$.



(a) Impact of probability of attempting transmission on π . (b) Impact of probability of attempting transmission on fraction of packets undergoing collisions.

Figure 4.13: Impact of probability of transmission attempts in Bufferless MACs.

Figure 4.13(a) shows the impact of the probability of attempting a transmission (when in possession of a packet) on π when $\lambda = \frac{1}{5000}$ and $L = 50$ slots. We observe a decrease in π when β increases from $\frac{1}{16}$ to $\frac{1}{8}$. This occurs in broadcast networks where there are no retransmissions as increasing β increases the rate at which the MAC layer is able to service the arrivals from the higher layers. In Figure 4.11, and Figure 4.13, we observe that adapting the packet generation rates at the higher layers has a higher impact on π and P_{coll} as compared to adapting β , the probability at which the MAC layer attempts a transmission when in possession of a packet. Similarly, in Figure 4.12, and Figure 4.13 we observe that adapting the size of packets at the application layer, or the data rate at which the messages are transmitted over the air at the MAC layer, have a greater impact of π and P_{coll} compared to adapting β .

These observations can be interpreted in the following ways:

1. Reducing the rate of packet generation from once every 2500 slots (50 milliseconds) to once every 5000 slots (100 milliseconds) reduces the fraction of packets lost due to collisions. Hence, minimising the rate at which packets are generated at the application layer is essential to keep a control on the fraction of packets lost due to collisions.
2. Reducing the number of slots for which the data is transmitted over the air

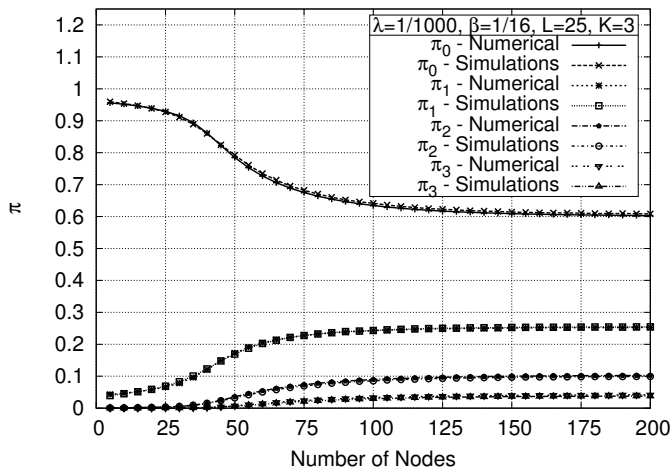


Figure 4.14: Probability of finding a node in State i ($0 \leq i \leq K$) when $K = 3$.

reduces the fraction of packets lost due to collisions. Hence, techniques like transmission of the whole certificate in alternate packets, as proposed in [9] and using signing algorithms that have smaller bandwidth overheads (increase in packet size) can be used to keep packet losses due to collision under control. Further, transmitting packets at higher data rates at the MAC layer can be used to keep packet losses due to collisions under control.

We now discuss the simulation results when there are no restrictions on the packet generation rates. We varied the buffer size from 3 to 10 to study the impact of buffer size on the performance on broadcast communication. Figure 4.14 shows the steady probability of finding a node with i packets in its buffers when the MAC layer has a buffer size (K) of 3 packets, $\lambda = \frac{1}{1000}$, $\beta = \frac{1}{16}$, and $L = 25$ slots. We observe that the probability of having at least one packet ($1 - \pi_0$) increases with node density.

Figure 4.15 shows the impact of packet generation rates on the steady state probability of not having even one packet in the buffers (π_0) and the fraction of packets undergoing collisions when $\beta = \frac{1}{16}$, $L = 25$ slots and $K = 3$ packets. Figure 4.15(a) shows that increasing the rate of arrivals from $\frac{1}{1000}$ to $\frac{1}{500}$ reduces the probability of finding a node in State 0. This results in an increase in the number of packets undergoing collisions as shown in Figure 4.15(b). Similarly, Figure 4.16(a) shows that increasing β from $\frac{1}{16}$ to $\frac{1}{8}$ when $\lambda = \frac{1}{500}$, $L = 25$ slots and $K = 3$, increases the

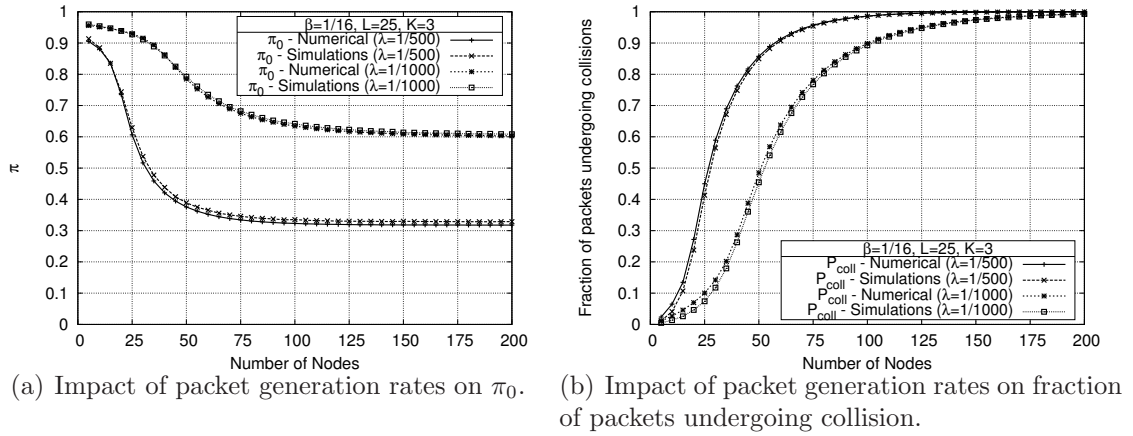


Figure 4.15: Impact of packet generations rates in systems with finite buffers.

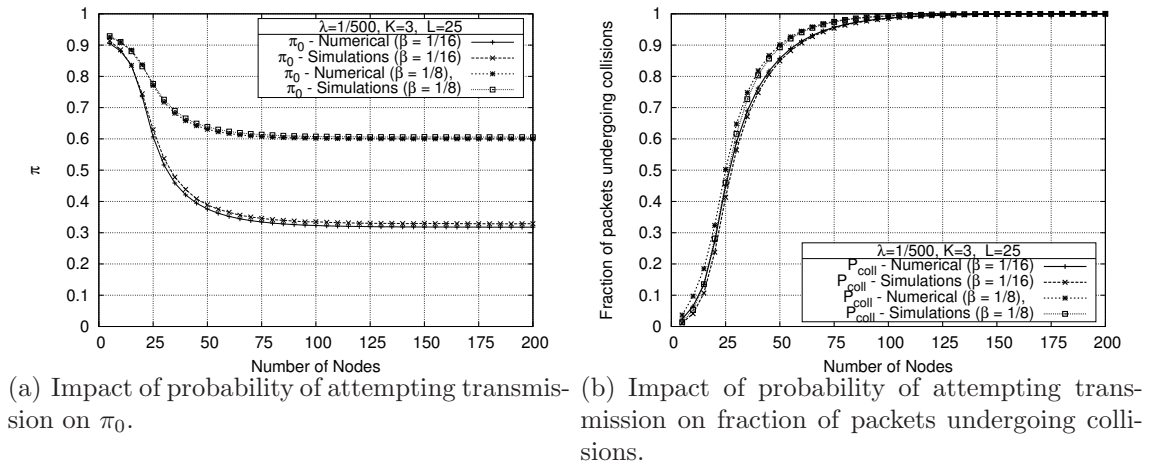


Figure 4.16: Impact of probability of transmission attempts in systems with finite buffers.

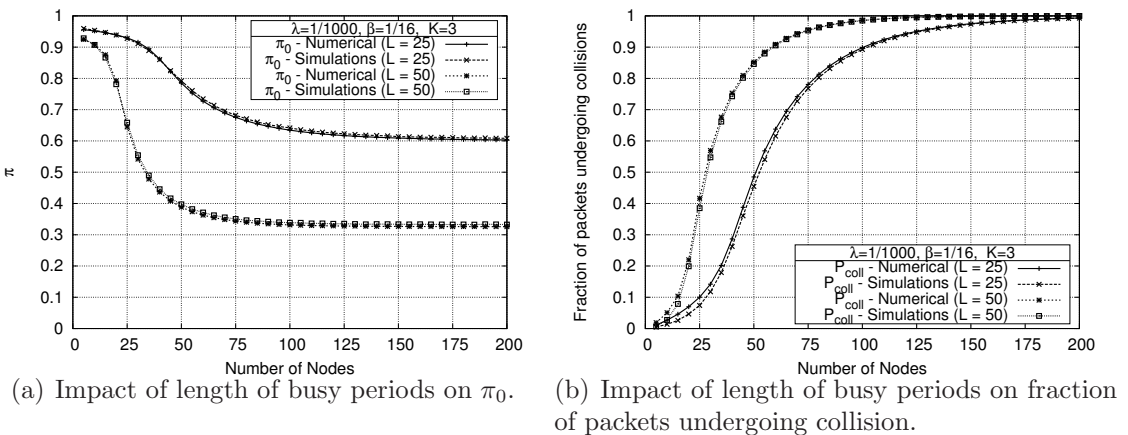


Figure 4.17: Impact of length of busy periods in systems with finite buffers.

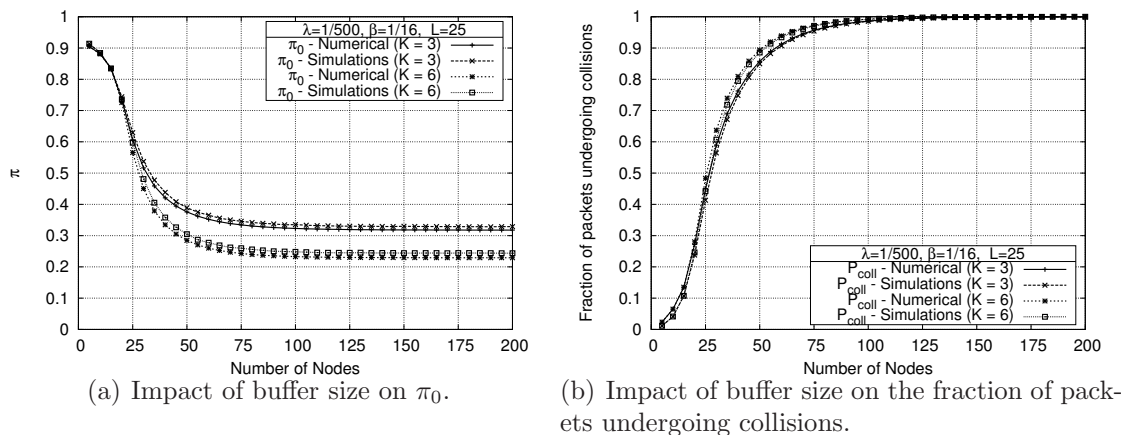


Figure 4.18: Impact of buffer size in systems with finite buffers.

probability of finding a node in State 0. In Figure 4.15(a) and Figure 4.16(a), we observe that for a given value of system parameters, λ , β , L , and K , π_0 converges for large values of node density. This value corresponds to the value of π_0 when $P_{coll} = 1$. Further, we observe that adapting the packet arrival rates from the higher layers, have a greater impact on the collisions as compared to adapting the probability of attempting a transmission which is similar to our observations in the case of low arrival rates.

As in the case of low arrival rates, in Figure 4.17 we observe a similarity in adapting the busy period lengths and packet arrival rates. Further, we again observe that adapting the length of the busy periods and the packet arrival rates have a greater impact on fraction of packets lost due to collisions as compared to adapting the probability of transmission attempt. When $\lambda = \frac{1}{500}$ (which corresponds to generating packets once every 10 milliseconds), $\beta = \frac{1}{16}$ and $L = 25$ slots, we observe that increasing the buffer size (K) from 3 packets to 6 packets increases reduces the packets that were dropped, thus reducing π_0 and increasing the fraction of packets lost due to collisions as shown in Figure 4.18. Rao *et al.* [51], attempt to study the stability of the system and show that *large collision probability is good for the stability* of the system which is not the case when there are retransmissions.

4.4 Summary

In this chapter we highlighted the overheads due to security and studied the communication performance considering the impact of the computational overheads of security. Given the current delays in signing and verifying the messages, we showed that packet transmission and not packet processing is the bottleneck for CCW applications. This work was extended by Iyer *et al.* [34], to show that performance bottlenecks could shift from the security layer to the MAC layer and vice-versa depending on the system parameters. We then studied the performance of broadcast communication in vehicular networks and showed that adapting packet arrival rates from the application layer and the time for which the packet is transmitted over the air have a greater impact on the packet collisions as compared to adapting the probability of attempting a packet transmission and adapting the buffer size at the MAC layer.

Chapter 5

Conclusions and Future Work

In this chapter we summarize the work presented in this thesis and outline further research avenues.

5.1 Summary and Conclusion

The intermittent connectivity between the principals of vehicular networks and security infrastructure results in incomplete revocation information at the recipients of signed messages. This incomplete information puts the recipients of signed messages in a dilemma while accepting messages signed using certificates that are not present in the CRLs at the On Board Unit (OBU). We present a metric called Confidence on Security infrastructure that quantifies the confidence the recipients can have while accepting messages signed using certificates that are not present in the CRLs at the OBU. We then propose an accept/drop technique at the security layer called *Freshness Checks* aimed at minimising the impact of the delays in dissemination of revocation information. When certificate revocation occurs only due to faults we show that:

1. The rate of communicating with the infrastructure, for updating the revocation information in case of CRL based schemes or performing checks in case of the Freshness Check scheme, need not scale up as the density of vehicles present in the vehicular networks increases.
2. The Freshness Check scheme introduces False Negatives, which are not present in the CRL base schemes, hence CoS is not a good metric to compare the performance of the CRL based schemes and Freshness Check based scheme.
3. The Freshness Check scheme can provide a higher fraction of True Positives compared to the CRL based scheme when the infrastructure presence is low.

Thus, making them suitable for applications that are capable of tolerating a low fraction of True Positives while keeping the rate of communication with the infrastructure (or infrastructure density) low.

Further, when misbehavior occurs due to intentional malicious activities, then we show that an increase in vehicle density requires an increase in the rate of communication with the infrastructure.

The computational overheads of security due to the signing and verification operations at the source result in queuing at the security layer. Given the current delays involved in signing and verifying messages we show that packet processing and not packet transmission is a bottleneck. The safety applications for vehicular networks rely heavily on the broadcast services of the MAC layer. We show that rather than adapting the buffer size and probability of transmission attempt in a given slot, the following techniques are more beneficial in controlling the packet losses due to collisions.

1. Lowering the rate of generating packets at the application layer.
2. Reducing the packet sizes by reducing the amount of data exchanged in a packets and reducing the bandwidth overheads of security. This can be achieved by techniques like transmission of the whole certificate in alternate packets, as proposed in [9], and using signing algorithms that have smaller bandwidth overheads (increase in packet size).
3. Increasing the rate at which the data is transmitted over the air by the MAC layer.

5.2 Future work

Obtaining the rate of revocation is essential for determining the security performance and the rate of communication with the infrastructure. When the infrastructure relies on reports of misbehavior from the principals of vehicular networks, then the rate of communication with the infrastructure can affect the rate at revocation. Thus,

obtaining the rate of revocation becomes critical to evaluate the security performance of vehicular networks.

We proposed and analysed the performance of a hard accept/drop mechanism for the Freshness Checks schemes, where the recipients accept packets only if the source performed Freshness Checks in the last T_f (Freshness Check Threshold) units of time. This criteria can be relaxed by allowing the nodes to accept packets that were signed using certificates whose Freshness Checks were not performed in the last T_f time units, and based on a probability distribution. We currently compare the CRL based scheme and the Freshness Check scheme using Fraction of True Positives as metric for comparison. One can also resort to other strategies such as comparison using the total bytes exchanged between the infrastructure and the principals of vehicular networks.

We assumed deterministic arrival of packets while studying the impact of computational overheads of security. Studying the impact of various distributions for arrival of messages from the application layer and service of packets at the security layer is essential if one needs to analyze the queuing system for various security algorithms. Further, this work can be extended for studying the impact of priority queues at the security layer on the communication performance.

We do not have a closed form expression for the fraction of packets undergoing collisions. We have not performed any sensitivity analysis which is essential to obtain the best tunable parameter under a given set of conditions. Further, our analysis can be extended to priority queues at the MAC layer.

Finally, the impact malicious activities such as change in packet generation rates at the application layer on the security performance and communication performance needs to be analysed.

References

- [1] “<http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/camp3/pages/vscc.htm>.”
- [2] “<http://www.car-to-car.org/>.”
- [3] “<http://www.isi.edu/nsnam/ns/>.”
- [4] “<http://www.network-on-wheels.de/>.”
- [5] “<http://www.path.berkeley.edu/>.”
- [6] “<http://www.sevecom.org/>.”
- [7] “Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” ASTM, 2003.
- [8] *IEEE Std 802.11e-2005, 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*, 2005.
- [9] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE Std 1609.2-2006*, 2006.
- [10] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, IEEE Std 1609.4-2006*, 2006.
- [11] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Resource Manager, IEEE Std 1609.1-2006*, 2006.
- [12] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, IEEE Std 1609.3-2007*, 2007.
- [13] *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*, June 12 2007.
- [14] C. Adams and R. Zuccherato, “A General, Flexible Approach to Certificate Revocation,” Entrust Inc, Tech. Rep., 1998.
- [15] N. H. S. Administration, “Vehicle Safety Communication Project, Final Report,” U.S. Department of Transportation, Tech. Rep. DOT HS 810 591, April 2006.

- [16] A. Aijaz, B. Bochow, F. Dotzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmuller, "Attacks on Inter Vehicle Communication Systems - an Analysis," *Int'l Workshop on Intelligent Transportation (WIT)*, 2006.
- [17] F. Bai, N. Sadagopan, and A. Helmy, "IMPORTANT: a framework to systematically analyze the Impact of Mobility on Performance of Routing Protocols for Adhoc Networks," *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies.*, pp. 825–835 vol.2, 30 March-3 April 2003.
- [18] F. Bai, H. Krishnan, V. Sadekar, G. Holland, and T. ElBatt, "Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective," in *1st IEEE Workshop on Automotive Networking and Applications (AutoNet 2006)*, 2006.
- [19] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE Journal on Selected Areas in Communications.*, vol. 18, no. 3, pp. 535–547, 2000.
- [20] S. Capkun, L. Buttyán, and J.-P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52–64, 2003.
- [21] X. Chen, H. H. Refai, and X. Ma, "Saturation performance of IEEE 802.11 broadcast scheme in ad hoc wireless lans," in *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, Sept. 30 2007-Oct. 3 2007, pp. 1897–1901.
- [22] J.-M. Choi, J. So, and Y.-B. Ko, "Numerical analysis of IEEE 802.11 broadcast scheme in multihop wireless ad hoc networks," *Information Networking*, pp. 1–10, 2005.
- [23] D. A. Cooper, "A more efficient use of delta-crls," *IEEE Symposium on Security and Privacy*, 2000.
- [24] M. Diffie, W.; Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, Nov 1976.
- [25] DSRC Industry Consortium, "DSRC Technology and the DSRC Industry Consortium (DIC) Prototype Team, White Paper," Tech. Rep., 2005.
- [26] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," *European Wireless*, 2002.
- [27] T. ElBatt, S. Goel, V. Kukshya, G. Holland, H. Krishnan, and J. Parikh, "Communications Performance Evaluation of Cooperative Collision Warning Applications," *IEEE Plenary Session, Task Group P*, July 2005.
- [28] T. ElBatt, S. K. Goel, G. Holland, H. Krishnan, and J. Parikh, "Cooperative collision warning using dedicated short range wireless communications," in *VANET '06: Proceedings of the 3rd international workshop on Vehicular ad hoc networks*. New York, NY, USA: ACM Press, 2006, pp. 1–9.

- [29] T. Freeman, R. Housley, A. Malpany, D. Cooper, and T. Polk, "Server-based Certificate Validation Protocol (SCVP)," *IETF Draft*, January 2007. [Online]. Available: <http://www.ietf.org/internet-drafts/draft-ietf-pkix-scvp-31.txt>
- [30] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in *VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. New York, NY, USA: ACM, 2004, pp. 29–37.
- [31] V. Goyal, "Fast digital certificate revocation, an alternative to short lived certificates," *Security and Protection in Information Processing Systems*, pp. 488–500, 2004.
- [32] R. Groenevelt, P. Nain, and G. Koole, "Message delay in manet," in *SIGMETRICS '05: Proceedings of the 2005 ACM SIGMETRICS international conference on Measurement and modeling of computer systems*. New York, NY, USA: ACM, 2005, pp. 412–413.
- [33] J.-P. Hubaux, S. Čapkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security and Privacy*, vol. 2, no. 3, pp. 49–55, 2004.
- [34] A. Iyer, A. Kherani, A. Rao, and A. Karnik, "Secure V2V Communications: Performance Impact of Computational Overheads," *IEEE Infocom 2008, Mobile Networking for Vehicular Environments workshop.*, 2008.
- [35] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," *International Journal of Information Security*, 2001.
- [36] D. Jungels, M. Raya, I. Aad, and J. Hubaux, "Certificate Revocation in Vehicular Ad Hoc Networks," *Security in Ad hoc and Sensor Networks (SASN)*, 2005.
- [37] P. C. Kocher, "On certificate revocation and validation," in *FC '98: Proceedings of the Second International Conference on Financial Cryptography*. London, UK: Springer-Verlag, 1998, pp. 172–177.
- [38] R. Kroh, A. Kung, and F. Kargl, "VANET Security Requirements: Initial Version," SEVECOM, Tech. Rep. IST-027795, July 2006.
- [39] A. Kumar, E. Altman, D. Miorandi, and M. Goyal, "New insights from a fixed-point analysis of single cell ieee 802.11 wlans," *IEEE/ACM Trans. Netw.*, vol. 15, no. 3, pp. 588–601, 2007.
- [40] D. Malone, K. Duffy, and D. Leith, "Modeling the 802.11 distributed coordination function in nonsaturated heterogeneous conditions," *IEEE/ACM Trans. Netw.*, vol. 15, no. 1, pp. 159–172, 2007.
- [41] P. McDaniel and A. D. Rubin, "A Response to "Can We Eliminate Certificate Revocation Lists?,"" in *FC '00: Proceedings of the 4th International Conference on Financial Cryptography*. London, UK: Springer-Verlag, 2001, pp. 245–258.

- [42] S. McDaniel, P.; Jamin, “Windowed certificate revocation,” *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 3, pp. 1406–1414, March 2000.
- [43] A. Menezes, P. Van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 2001. [Online]. Available: <http://www.cacr.math.uwaterloo.ca/hac/>
- [44] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP,” *Network Working Group, Request For Comments - 2560*, June 1999. [Online]. Available: <http://www.ietf.org/rfc/rfc2560.txt>
- [45] P. Papadimitratos, L. Buttyán, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, “Architecture for secure and private vehicular communications,” *Telecommunications, 2007. ITST '07. 7th International Conference on ITS*, pp. 1–6, June 2007.
- [46] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, “Securing Vehicular Communications - Assumptions, Requirements, and Principles,” in *Workshop on Embedded Security in Cars (ESCAR) 2006*, 2006. [Online]. Available: <http://www.escar.info/06/general.html>
- [47] B. Parno and A. Perrig, “Challenges in securing vehicular networks,” in *Proceedings of Workshop on Hot Topics in Networks (HotNets-IV)*, Nov 2005.
- [48] K. Plössl, T. Nowey, and C. Mletzko, “Towards a security architecture for vehicular ad hoc networks,” *First International Conference on Availability, Reliability and Security (ARES'06)*, 2006.
- [49] L. Qiu, Y. Zhang, F. Wang, M. K. Han, and R. Mahajan, “A general model of wireless interference,” in *MobiCom '07: Proceedings of the 13th annual ACM international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2007, pp. 171–182.
- [50] A. Rao, A. Sangwan, A. Kherani, A. Varghese, B. Bellur, and R. Shorey, “Secure V2V Communication With Certificate Revocations,” *IEEE Infocom 2007, Mobile Networking for Vehicular Environments workshop.*, pp. 127–132, 2007.
- [51] A. Rao, A. A. Kherani, and A. Mahanti, “Performance evaluation of 802.11 broadcasts for a single cell network with unsaturated nodes,” in *Networking*, 2008, pp. 836–847.
- [52] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, “On data-centric trust establishment in ephemeral ad hoc networks,” in *To Appear in IEEE Infocom Conference*, April. 2008.
- [53] 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, no. 1, pp. 39 – 68, 2007.

- [54] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks*, 2007.
- [55] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [56] R. Rivest, "Can We Eliminate Certificate Revocation Lists," *Financial Cryptography*, vol. 1465, pp. 178–183, 1998.
- [57] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "Amoeba: Robust location privacy scheme for vanet," *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 8, pp. 1569–1589, Oct. 2007.
- [58] K. Scheibelhofer, "PKI without Revocation Checking," *4th Annual PKI R&D Workshop*, 2005.
- [59] A. Slagell, R. Bonilla, and W. Yurcik, "A survey of pki components and scalability issues," *Performance, Computing, and Communications Conference, 2006. IPCCC 2006. 25th IEEE International*, pp. 10 pp.–, 10-12 April 2006.
- [60] W. Stadje, "The Busy Period of the Queueing System M/G/ ∞ ," *Journal of Applied Probability*, vol. 22, no. 3, pp. 697–704, 1985.
- [61] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Pearson Education, 2006.
- [62] H.-S. Tan and J. Huang, "DGPS-based vehicle-to-vehicle cooperative collision warning: Engineering feasibility viewpoints," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 7, no. 4, pp. 415–428, Dec. 2006.
- [63] The CAMP Vehicle Safety Communications Consortium, "Vehicle safety communications project task 3 final report identify: Intelligent vehicle safety applications enabled by DSRC," National Highway Traffic Safety Administration, U. S. Department of Transportation (USDOT), Tech. Rep. 809859, Mar. 2005.
- [64] M. Torrent-Moreno, M. Killat, and H. Hartenstein, "The challenges of robust inter-vehicle communications," in *Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd*, vol. 1, 2005, pp. 319–323.
- [65] M. Torrent-Moreno, S. Corroy, F. Schmidt-Eisenlohr, and H. Hartenstein, "IEEE 802.11-based one-hop broadcast communications: Understanding transmission success and failure under different radio propagation environments," in *MSWiM '06: Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems*. New York, NY, USA: ACM Press, 2006, pp. 68–77.
- [66] M. Torrent-Moreno, D. Jiang, and H. Hartenstein, "Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks," pp. 10–18, 2004.

-
- [67] P. Varaiya, "Smart cars on smart roads: problems of control," *Automatic Control, IEEE Transactions on*, vol. 38, no. 2, pp. 195–207, 1993.
- [68] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-vehicle safety messaging in DSRC," in *VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. New York, NY, USA: ACM Press, 2004, pp. 19–28.
- [69] X. Yang, L. Liu, N. H. Vaidya, and F. Zhao, "A vehicle-to-vehicle communication protocol for cooperative collision warning," in *Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004. The First Annual International Conference on*, 2004, pp. 114–123.
- [70] J. Yin, T. ElBatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, and T. Talty, "Performance evaluation of safety applications over dsrc vehicular ad hoc networks," in *VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. New York, NY, USA: ACM Press, 2004, pp. 1–9.
- [71] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security Issues in a Future Vehicular Network," *Proceedings Of European Wireless*, 2002.

Appendix A

Simulating Security Overheads

In Section A.1 we provide a brief overview of the details of the changes done in the *ns2* simulator to incorporate the overheads of security. In Section A.2 we provide the algorithm used to simulate broadcast communication at the MAC layer.

A.1 Design for Security Layer in ns2

The abstraction of the periodic message arrival from the application layer and the processing overheads of the cryptographic server is done using 2 timers; T_1 for periodic generation of packets and T_2 for abstracting the time spent at the cryptographic server.

The activities carried on the expiry of the T_1 timer are as follows:

1. Add the element to the security queue.
2. If this is the only element in the security queue then set the cryptographic timer T_2 to expire after t_{ss} seconds.
3. Set the timer T_1 to timeout after t_p seconds.

The activities carried on the expiry of the T_2 timer are as follows:

1. If the packet is being served at the source then send the packet to the MAC Layer else send the packet to the application layer.
2. If queue is not empty then schedule the timer to expire after t_{ss} seconds if the first packet was generated by the application layer else schedule the time to expire after t_{sd} seconds.

The activities carried on reception of packet from the MAC layer are:

1. Add the element to the security queue.

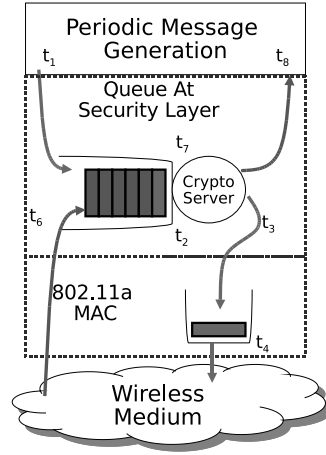


Figure A.1: Timing values stored in individual packets

2. If this is the only element in the security queue then set the cryptographic timer T_2 to timeout after t_{sd} seconds.

The details of the time spent at various queues is required for the analysis of the system. These values are stored in the packets along with the number of elements present in each queue when a packet arrives at that queue. Figure A.1 provides the details of the time values stored in each packet.

t_1 The time of packet generation which represents the time at which the packet arrives at the security queue of the source.

t_2 The time when the packet reaches the head of line of the security queue at the source of the message.

t_3 The time when the packet leaves security layer for the MAC layer of the source.

t_4 The time when the packet reaches the head of line of the MAC queue.

t_5 The time when the first bit is transmitted in the wireless medium.

t_6 The time when the packet arrives at the security queue of the destination.

t_7 The time when the packet reaches the head of line of the security queue at the destination.

t_8 The time when the packet leaves the cryptographic server for the application layer

The various events that can cause the packet to leave the system are:

1. The packet is dropped as the expiry time elapses while the packet is at the security layer of source or destination.
2. The packet undergoes collision in the wireless medium.
3. The packet reaches the application layer of the destination.

Figure A.2 provides the details of the trace file format used for obtaining the numerical results. This format is used to dump the details of the life-time of the packet whenever it leaves the system. The source id, sequence number and destination id are used to uniquely identify a packet.

Time of event	Event	Source id	Seq. No.	Dest. id	t_1	n_1	t_2	t_3	n_2	t_4	t_5	t_6	n_3	t_7	t_8	flag
---------------	-------	-----------	----------	----------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	------

Figure A.2: Trace File Format

A.2 Algorithm For Abstracting MAC Layer

The algorithm for abstracting the IEEE 802.11 MAC for broadcast traffic is given below. The inputs to the algorithm are:

1. The probability of transmission in a given slot β .
2. The probability of packet arrival in a given slot λ .
3. The total number of nodes in the cell n ($n \geq 2$)
4. The number of slots for which the channel is sensed busy L .
5. The number of buffers at the MAC layer (K).

Collisions occur only when more than 1 node attempt to transmit in a given cycle. It computes the probability of collision (P_{coll}) as the fraction of total transmitted packets undergoing collision after 10^6 cycles. At the beginning of each cycle it keeps track of the number of nodes that have a packet to transmit in that cycle. The value of π is obtained from this count at the end of the simulation.

Algorithm 1 Abstraction of IEEE 802.11 MAC For Broadcast Traffic

```

1: procedure ABSTRACTMAC( $L, \lambda, \beta, n, K$ )
2:    $C_p \leftarrow 0$  ▷  $C_p$ : Probability of Packet Collisions
3:    $T_x \leftarrow 0$  ▷  $T_x$ : Number of packet transmission attempts
4:   for  $i = 0$  to  $K$  do
5:      $Pi[i] \leftarrow 0$  ▷  $\pi$  is an array of size  $K + 1$ 
6:   end for
7:   for  $i = 1$  to  $n$  do
8:     if  $random(0, 1) \leq \lambda$ , then
9:        $Q[i] \leftarrow 1$  else  $Q[i] \leftarrow 0$  end if
10:  end for
11:  for  $cycle = 1$  to  $10^6$  do ▷ Repeat for 1 million cycles
12:    for  $i = 1$  to  $n$  do
13:      Increment  $Pi[Q[i]]$ 
14:    end for
15:     $t_x \leftarrow 0$  ▷ Number of transmitters in a cycle
16:    while  $t_x = 0$  do
17:      for  $i = 1$  to  $n$  do
18:         $Attempt[i] \leftarrow 0$ 
19:        if  $Q[i] > 0$  and  $random(0, 1) \leq \beta$  then
20:           $Attempt[i] \leftarrow 1$ ;  $t_x \leftarrow t_x + 1$ 
21:        end if
22:        if  $Q[i] < K$  and  $random(0, 1) \leq \lambda$  then
23:           $Q[i] \leftarrow Q[i] + 1$ 
24:        end if
25:      end for
26:    end while
27:    for  $slots = 1$  to  $L$  do
28:      for  $i = 1$  to  $n$  do
29:        if  $Q[i] < K$  and  $random(0, 1) \leq \lambda$ , then Increment  $Q[i]$  end if
30:      end for
31:    end for
32:    for  $i = 1$  to  $n$  do
33:      if  $Attempt[i] = 1$ , then  $Q[i] \leftarrow Q[i] - 1$  end if
34:    end for
35:     $T_x \leftarrow T_x + t_x$ 
36:    if  $\{t_x > 1\}$ , then  $C_p \leftarrow C_p + t_x$  end if ▷ Collisions if more than 1  $t_x$ 
37:  end for
38:   $C_p \leftarrow \frac{C_p}{T_x}$ 
39:  for  $i = 0$  to  $K$  do
40:     $\pi_i \leftarrow \frac{Pi[i]}{\sum_{i=0}^K Pi[i]}$ 
41:  end for
42: end procedure

```

Technical Biography of Author

Ashwin Rao received his B.E. in Computer Science from Pune Institute of Computer Technology (affiliated to the University of Pune) in May 2004. From July 2004 to July 2006 he was working with AirTight Networks Inc., Pune as a Member of Technical Staff. Since July 2006, he is enrolled in the Master of Science (by Research) program in the Amar Nath and Shashi Khosla School of Information Technology at the Indian Institute of Technology Delhi.

Refereed Publications:

1. A. Rao, A. Sangwan, A. Kherani, A. Varghese, B. Bellur, and R. Shorey, "Secure V2V Communication With Certificate Revocations," *IEEE Infocom 2007, Mobile Networking for Vehicular Environments workshop.*, pp. 127–132, 2007.
2. A. Iyer, A. Kherani, A. Rao, and A. Karnik, "Secure V2V Communications: Performance Impact of Computational Overheads," *IEEE Infocom 2008, Mobile Networking for Vehicular Environments workshop.*, 2008.
3. A. Rao, A. A. Kherani, and A. Mahanti, "Performance Evaluation of 802.11 Broadcasts for A Single Cell Network with Unsaturated Nodes," in *Networking*, 2008, pp. 836–847.
4. A. Kherani and A. Rao, "Security-Performance of Node Eviction Schemes in Vehicular Networks", manuscript submitted to *IEEE Transactions on Vehicular Technology* on September 27, 2008