PERFORMANCE EVALUATION OF A SECURE MAC PROTOCOL FOR VEHICULAR NETWORKS

Yi Qian [1], Kejie Lu [2], and Nader Moayeri [1]

[1] National Institute of Standards and Technology
100 Bureau Drive, Stop 8920
Gaithersburg, MD 20899-8920, USA

[2] Department of Electrical and Computer Engineering
University of Puerto Rico
Mayaguez, PR 00681, USA

ABSTRACT *The main benefit of vehicular communication is seen in active safety systems that increase passenger safety by exchanging warning messages between vehicles. Other applications and private services are also permitted in order to lower the cost and to encourage vehicular network deployment and adoption. The allocation of 75 MHz in the 5.9 GHz frequency band licensed for Dedicated Short Range Communications (DSRC), which supports seven separate channels, may also enable the future delivery of rich multimedia contents to vehicles at short- to medium-range via vehicular communications. There are many challenges that must be addressed before vehicular networks can be successfully deployed. Among these challenges is designing of security mechanisms to secure vehicular networks against abuse, and designing of efficient medium access control (MAC) protocols so that safety related and other application messages can be timely and reliably disseminated through vehicular networks. In this paper, we give an overview on a priority based secure MAC protocol for vehicular networks and present detailed security and performance analysis. We show that the MAC protocol can achieve both QoS and security requirements for vehicular network safety applications.*

1. INTRODUCTION

Vehicular networks have been developed to improve the safety, security and efficiency of the transportation systems and enable new mobile applications and services for the traveling public. The field of inter-vehicular communications (IVC), including both vehicle-to-vehicle communications (V2V) and vehicle-to-roadside communications (V2R), is recognized as an important component of the much needed overhaul of the highway information system infrastructure. The immediate impacts include alleviating the vehicular traffic congestions and improving operation management in support of public safety goals, such as collision avoidance. Equipping vehicles with various kinds of on-board sensors, and V2V and V2R communication capabilities, will allow large-scale sensing and decision / control actions in support of these objectives. Communication-based active safety is viewed as the next logical step towards proactive safety systems. These systems provide an extended information horizon to warn the driver or the vehicle of potentially dangerous situations at an early stage. The allocation of 75 MHz in the 5.9 GHz frequency band licensed for DSRC in North America, which supports seven separate channels, may also enable the future delivery of rich multimedia contents to vehicles at short- to medium-range via either V2V or V2R vehicular network links [1] [2].

Many research challenges must be fully studied before vehicular networks can be successfully deployed. Among them is the design of a secure medium access control (MAC) protocols that can make best use of DSRC multichannel architecture, and schedule application packet transmissions fairly and securely in vehicular networks, according to the quality of service (QoS) and security requirements of the applications. In this paper, we give an overview on a secure MAC protocol for vehicular networks, with different message priorities for different types of applications to access DSRC channels [3], and then present detailed security analysis and performance analysis on the protocol. We show by analysis and simulations that the MAC protocol can achieve both security and QoS requirements for vehicular network safety applications.

In the rest of this paper, in Section 2 we first give a brief overview on vehicular networks and the description of the secure MAC protocol. We present our security analysis of the protocol in Section 3, followed by a detailed simulation and performance analysis in Section 4. Conclusions are given in Section 5.

2. BACKGROUND ON VEHICULAR NETWORKS AND A SECURE MAC PROTOCOL

2.1. BASICS ON VEHICULAR NETWORKS

In a vehicular network, each vehicle is equipped with the technology that allows the vehicle to communicate

with each other as well as with the roadside infrastructure, e.g., base stations also known as roadside units (RSUs), located in some critical sections of the road, such as traffic lights, intersections, or stop signs, to improve the driving experience and make driving safer. By using such communication devices, also known as on-board units (OBUs), vehicles can communicate with each other as well as with RSUs. A vehicular network is a self-organized network that enables communications between vehicles and RSUs, and the RSUs can be connected to a backbone network, so that many other network applications and services can be provided to the vehicles. Figure 1 shows an example of a vehicular network.

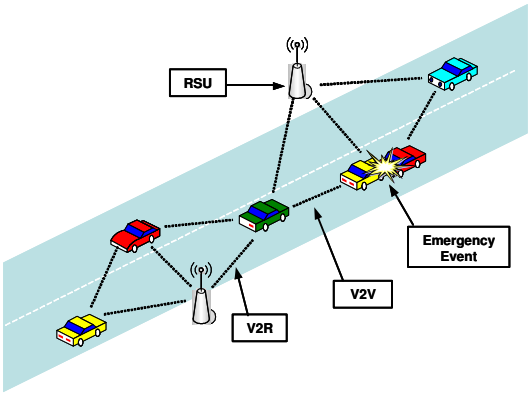

Figure 1. An example of a vehicular network

The U.S. Federal Communications Commission (FCC) recently allocated 75 MHz of DSRC spectrum at 5.9 GHz to be used exclusively for V2V and V2R communications [1]. The primary purpose is to enable public safety applications that save lives and improve vehicular traffic flow. Private services are also permitted in order to lower the network deployment and maintenance costs to encourage DSRC development and adoption. The DSRC spectrum is divided into seven 10-MHz wide channels as shown in Figure 2. Channel 178 is the control channel, which is generally restricted to safety communications only. The two channels at the edges of the spectrum are reserved for future advanced accident avoidance applications and high-power public safety communication usages. The rest are service channels and are available for both safety and non-safety applications.

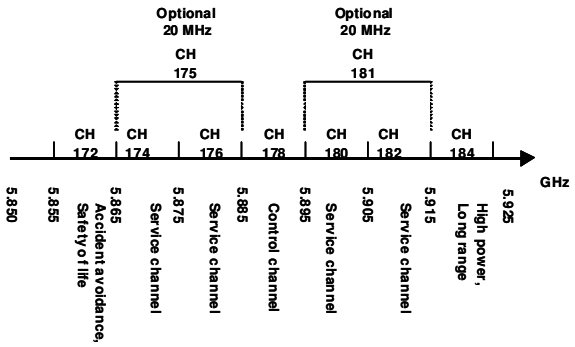

Figure 2. DSRC Channel assignment in North America

In the following we summarize the existing applications and several potential applications that have been proposed for vehicular networks. As studied in [4] and [5], vehicular networks would support life-critical safety applications, safety warning applications, electronic toll collection, Internet access, group communications, roadside service finder, etc. In [5] we have also elaborated on the functions of each application that shall be provided in the MAC layer and the network layer, so as to fulfill the requirements of these applications.

Table 1 lists the characteristics of the example vehicular network applications discussed in [5], with the priorities of the application message classes, allowable latency as the major QoS requirements of the applications, the network traffic types, and the message transmission ranges.

Table 1. Example vehicular network applications

Applications	Priority	Allowable Latency (ms)	Network Traffic Type	Message Range (m)
Life-Critical Safety	Class 1	100	Event	300
Safety Warning	Class 2	100	Periodic	50 - 300
Electronic Toll Collection	Class 3	50	Event	15
Internet Access	Class 4	500	Event	300
Group Communications	Class 4	500	Event	300
Roadside Service Finder	Class 4	500	Event	300

For safety messages, the amount of information to be transmitted is relatively small, but the transmission reliability as well as the latency and packet dissemination are of great importance.

The IEEE has completed the standards IEEE P1609.1, P1609.2, P1609.3, and P1609.4 for vehicular networks and recently released them for trial use [6]. P1609.1 is the standard for the Wireless Access for Vehicular Environments (WAVE) Resource Manager. It defines the services and interfaces of the WAVE resource manager

application as well as the message data formats. It provides access for applications to the other architectures. P1609.2 defines security, secure message formatting, processing, and message exchange. P1609.3 defines routing and transport services. It provides an alternative to IPv6. It also defines the management information base for the protocol stack. P1609.4 deals mainly with specification of the multiple channels in the DSRC standard.

The WAVE stack uses a modified version of the IEEE 802.11a, known as IEEE 802.11p [7], for its Medium Access Control (MAC) layer protocol. It uses CSMA/CA as the basic medium access scheme for link sharing and uses one control channel to set up transmissions, which then are carried over some transmission channels. The 802.11p PHY layer is expected to work in the 5.850 – 5.925 GHz DSRC spectrum in North America, which is a licensed Radio Services Band in the United States. By using the OFDM system, it provides both V2V and V2R wireless communications over distances up to 1000 m, while taking into account the environment, that is, high absolute and relative velocities (up to 200 km/h), fast multipath fading and different scenarios (rural, highway, and urban). Operating in 10-MHz channels, it should allow data payload communication rates of 3, 4, 5, 6, 9, 12, 18, 24, and 27 Mb/s. By using the optional 20 MHz channels, it allows data payload capabilities up to 54 Mb/s.

2.2. THE SECURE MAC PROTOCOL FOR VEHICULAR NETWORKS

In the past few years, considerable effort has been spent in research on vehicular networking protocols and applications. However, research on security threats and solutions of vehicular networks started only recently. While most of the previous studies on vehicular network security concentrate on particular security mechanisms and solutions on vehicular network communications (e.g., [3], [8-11]), there are not many works on secure medium access control.

In this subsection we give an overview on the secure MAC protocol that we proposed recently in [3], which in consideration of the DSRC channel structures, and to accommodate the DSRC applications while providing adequate security for vehicular networks. The proposed secure MAC protocol will use part of the IEEE 1609.2 security infrastructure including PKI and ECC, the secure communication message format for vehicular networks, and the priority based channel access according to the QoS requirements of the applications.

As shown in Figure 2, the two channels at the edges of the spectrum (Ch 172 & Ch 184) are reserved for future DSRC applications. We assume here that there are four internal queues per OBU for the four different priority message classes, and each message will be queued in a queue according to its priority. Class 1 message will always access the channel 178 with the highest priority, if the channel 178 is full, then it will access either of the channels 174, 176, 180, or 182 with the highest priority; Class 2 message will always access the channel 178 with the 2nd highest priority, if the channel 178 is full, then it will access either of the channels 174, 176, 180, or 182 with the 2nd highest priority; Class 3 and Class 4 message cannot access the channel 178, and it will access channels 174, 176, 180, or 182 with the 3rd or 4th priority respectively. We assume that there is a scheduler in each OBU, which handles the internal collision. The scheduler will allow higher priority messages to be transmitted before lower priority messages. We adopt a preemptive policy, that an arriving high priority (Class 1 and Class 2) safety related message will be scheduled to get the channel immediately before the completion of the current low priority (Class 3 and Class 4) message transmission. Table 2 shows the traffic priority classes and the DSRC channels that each class can access.

Table 2. Message Priority Classes and the DSRC Channels

Message Priority Classes	DSRC Channels
Class 1	178, 174, 176, 180, and 182
Class 2	178, 174, 176, 180, and 182
Class 3	174, 176, 180, and 182
Class 4	174, 176, 180, and 182

As it is discussed in [5], vehicular network security requires message authentication and integrity, message non-repudiation, entity authentication, access control, message confidentiality, availability, privacy and anonymity, and liability identification for the safety related applications (Class 1 and Class 2).

For non-safety related messages (Class 3 and Class 4), different security requirements may be established as compared to those of Class 1 and Class 2. We assume that other security mechanisms will address the security requirements of Class 3 and Class 4 messages. We will focus our study in this paper on the impact of secure safety messages and the priority based medium access control mechanism for all DSRC applications.

Similar to [9], [10], and [11], we assume that each OBU on a vehicle has a secure database, which stores all cryptography components used for signing and verifying each message. Each vehicle has to have a valid certificate usually issued by a central trusted party called Certificate Authority (CA). PKI will be used for certificates issued by a CA. For the privacy of a vehicle, such as identity and travel route, a set of anonymous keys can be used to sign each message that will be changed periodically. These keys can be preloaded in the secure database of the OBU for a long period of time, e.g., for one year until next yearly license plate registration. Each key is certified by the issuing CA and has a short lifetime. In case of an accident or other law investigation, the authority can track back to the real identity of the vehicle, using Electronic License Plate (ELP) [8]. This can also help to prevent non-repudiation in case of accidents.

For safety related (Class 1 and Class 2) messages, message authentication and integrity, message non-repudiation, and privacy and anonymity of the senders are very important. Confidentiality of the safety message itself is not needed, so it can be transmitted in plaintext [9], [11]. Under the PKI solution, before an OBU sends a safety message, it signs it with its private key and includes the CA's certificate as follows:

$$V \rightarrow *: M, T, Sig_{PrKv}\{H[M|T]\}, Cert_V \quad (1)$$

where, V is the sender of the safety message, * represents any receivers, M is the safety message sent by plaintext, T is the time-stamp to guarantee the freshness of the message (is also sent in plaintext), $Sig_{PrKv}\{H[M|T]\}$ is the hash of the message M and time-stamp T, signed by the private key of the sender K_V, and $Cert_V$ is the pre-stored certificate of the sender issued by any CAs.

3. SECURITY ANALYSIS

Message authentication and integrity means that messages must be protected from any alteration and the receiver of a message must corroborate the sender of the message. But integrity does not necessarily imply identification of the sender of the message. Note that attackers cannot alter both message and time-stamp, due to digital signature. Since no other OBU knows the private key of the sender, no other OBU can alter the content in the packet. The certificate of the sender is included in the packet, so that other vehicles can extract the sender's public key and verify the correctness of each message. Once other OBUs receive a message, they retrieve the sender's public key, K_V from $Cert_V$ in order to decrypt the signature to obtain H[M|T], hash the message and time-stamp, compare the hash with H[M|T] and if both of them are the same, the message is verified. Otherwise the message is falsified and will be ignored. Therefore we can insure the message authentication and integrity in this protocol.

Message non-repudiation means that the sender of a message cannot deny having sent the message. In this protocol a vehicle cannot claim to be another vehicle because all the messages it transmitted were signed by its public keys. A vehicle cannot deny having sent a message because it is signed by an anonymous key that belongs exclusively to the sender. Also the vehicle cannot claim that the message was replayed because a timestamp is included in each message. Therefore the proposed MAC protocol can achieve message non-repudiation.

Privacy and anonymity of the senders means that conditional privacy must be achieved in the sense that the user-related information has to be protected from unauthorized access, while the authorities should be able to access such information to look for witnesses in case of a dispute such as a crime/car accident scene investigation. The user-related information includes the driver name, license plate, speed, position, and traveling routes. In [10] the authors have proposed a comprehensive design for a secure and privacy-preserving protocol based on group signature and identity (ID)-based signature techniques. The proposed protocol in [10] not only can guarantee the requirements of security and privacy, but also can provide the desired traceability of each vehicle in the case where the ID of the message sender has to be revealed by the authority for any dispute event. In our future work, we will show that our proposed secure MAC protocol can combine with [10] to achieve privacy and anonymity of vehicular networks.

4. PERFORMANCE ANALYSIS

In this section we present our simulation and analysis to show the performance results of the proposed secure MAC protocol. There are two scenarios of the vehicular networks: V2R based vehicular networks, and V2V based vehicular networks. In V2R based vehicular networks, we assume that the vehicular communication is controlled by RSUs. Each RSU acts as an access point that broadcasts all the messages received from one vehicle to all others in the range. In V2V based vehicular networks, on the other hand, we assume there is no RSU infrastructure exists, each OBU on a vehicle has to rely on its own for communications. It has to broadcast messages to all the nearby nodes. There is no acknowledgement in the V2V based vehicular network, unlike in the V2R based vehicular network where acknowledgement is created by

the RSU. In the following we show the performance of V2R based vehicular network secure communication scenario (Figure 5).

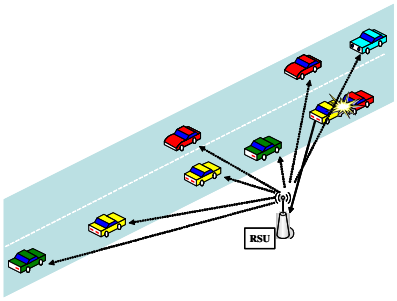

Figure 5. A V2R based vehicular network

In our simulation, we assume that each vehicle has five interface cards, each of which is operating on a different frequency band. Moreover, for each channel, we consider the 10-MHz channelization. In particular, the basic rate of the channel is 3 Mbps, the data rate of the channel is 5 Mbps. The channel medium access scheme is the same as that of the basic IEEE 802.11 DCF. In addition, we assume that the minimum window size is 31, the maximum window size is 1023, and the retry limit is 5.

In Figure 6 and Figure 7, we investigate the impact of the packet size, where we assume that the number of nodes in the network is fixed to 50 and the channel bit error rate is 10^{-5}, which is a practical scenario in wireless communication. We also assume that the packet arrival of each class of traffic on every node is exponential with average interval time being 50 ms.

Figure 6 illustrates the throughput versus packet size in bytes. We can clearly observe the differentiation of different Classes. For instance, when the packet size is small, which implies that the traffic is low, traffic of all Classes can be delivered in the network. And consequently the throughput increases linearly with the increase of packet size. However, if the packet size is greater than a certain threshold, throughput of Class 4, 3, and 2 will decline and gradually approaching 0. In contrast, the throughput of Class 1 traffic keeps increasing until the packet size reaches about 1700 Bytes. If the packet size is beyond this value, we can see that the throughput is less than the maximum and remains rather stable with the increase of the packet size. This indicates that the network has reached a saturation condition.

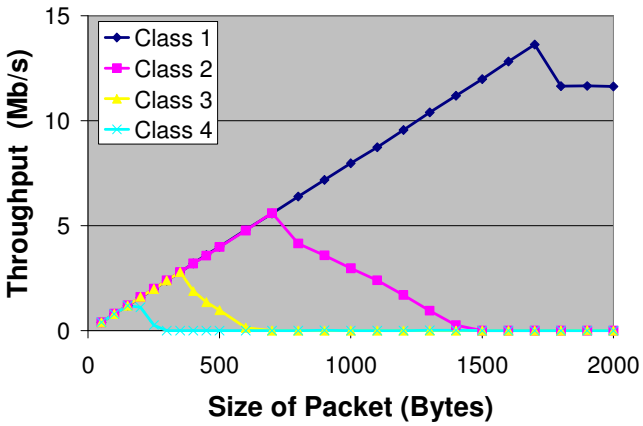

Figure 6. Throughput vs. packet size

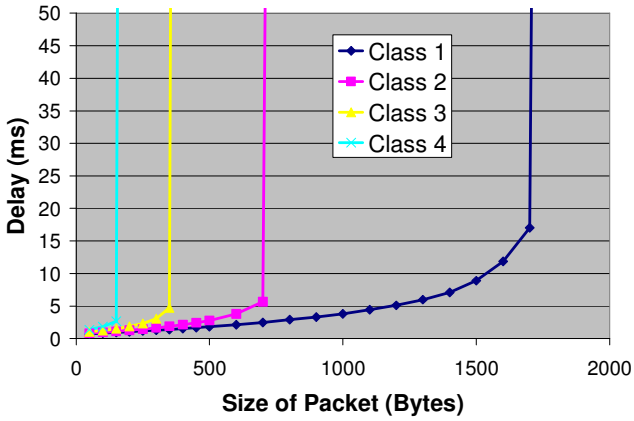

Figure 7. Delay vs. packet size

Notice that in the above experiment we assume that the transmission experiences 10^{-5} bit error rate. Nevertheless, in our experiments, we have also observed similar trends for other bit error conditions. The main difference in different tests is the maximum throughput and the corresponding packet size. Therefore, we will not present results for other bit error conditions.

The corresponding delay performance for Figure 6 is shown in Figure 7. Here we can observe that the delay performance of each class increase gradually with respect to the increase of the packet size, until the packet size reaches a certain value, which appeals to be the packet size that leads to the maximum throughput.

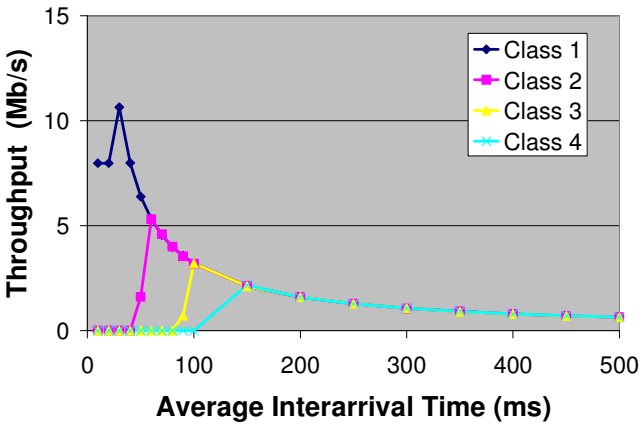

Figure 8. Throughput vs. average inter-arrival time

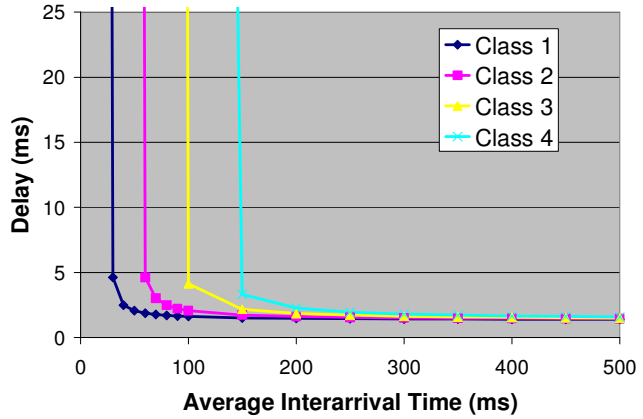

Figure 9. Delay vs. average inter-arrival time

In Figures 8 and 9, we illustrate the throughput and delay performance versus the average inter-arrival time. In this experiment, we consider that the number of nodes is 80 and the packet size is fixed to 500 Bytes. Similar to the previous experiment in Figures 6 and 7, we can see that Class 1 traffic has the first priority if the network load is large. And with the increase of inter-arrival time, the overall throughput decreases as expected.

5. CONCLUSIONS

Vehicular ad hoc networking is a promising wireless communication technology for improving highway safety and information services. In this paper we proposed a secure MAC protocol for vehicular networks with different message priorities for different types of applications to access DSRC channels. The secure communication protocol is designed to guarantee the freshness of the message, message authentication and integrity, message non-repudiation, and privacy and anonymity of the senders. Simulations results show that the proposed MAC protocol can provide secure communications while guarantee the QoS requirements of safety related vehicular network DSRC applications. Future work is continuing on the performance of V2V based secure communication scenario.

REFERENCES

[1] Dedicated Short Range Communications (DSRC) Home. http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

[2] Crash Avoidance Metric Partnership, "Vehicle Safety Communication Project Final Report", available through U.S. Department of Transportation.

[3] Yi Qian, Kejie Lu, and Nader Moayeri, "A Secure VANET MAC Protocol for DSRC Applications", Proceedings of *IEEE Globecom'2008*, New Orleans, LA, November 30 – December 4, 2008.

[4] Qing Xu, Tony Mak, Jeff Ko, and Raja Sengupta, "Vehicle-to-Vehicle Safety Messaging in DSRC", Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks (VANET'04), October 1, 2004, Philadelphia, PA.

[5] Yi Qian, and Nader Moayeri, "Design Secure and Application-Oriented VANETs", Proceedings of IEEE *VTC'2008-Spring*, Singapore, May 11-14, 2008.

[6] IEEE Draft P1609.0/D01, February 2007.

[7] IEEE Draft P802.11p/D2.0, November 2006.

[8] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, October 2006.

[9] Maxim Raya, and Jean-Pierre Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security, Vol.15, No.1, pp.39-68, 2007.

[10] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications", IEEE Transactions on Vehicular Technology, Vol.56, No.6, pp.3442-3456, November 2007.

[11] Chakkaphong Suthaputchakun, and Aura Ganz, "Secure Priority Based Inter-Vehicle Communication MAC Protocol for Highway Safety Messaging", Proceedings of IEEE ISWCS 2007, October 16-19, 2007, Trondheim, Norway.