A SECURE VANET MAC PROTOCOL FOR DSRC APPLICATIONS

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 — **Vehicular ad hoc networking is an important component of Intelligent Transportation Systems. The main benefit of vehicular ad hoc network (VANET) 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 VANET deployment and adoption. Dedicated Short Range Communications (DSRC) is a key enabling technology for VANET applications and services. There are many challenges that must be addressed before VANETs can be successfully deployed. Among these challenges is designing of security mechanisms to secure VANETs 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 VANETs. In this paper we propose a secure MAC protocol for VANETs, with different message priorities for different types of applications to access DSRC channels. Our simulations and analysis show that the proposed MAC protocol can provide secure communications while guarantee the reliability and latency requirements of safety related DSRC applications for VANETs.**

Keywords: **VANET, security, safety, MAC, DSRC.**

1. INTRODUCTION

Intelligent Transportation Systems (ITS) 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), also known as VANET, is recognized as an important component of ITS in various national plans [1]. The ITS architecture provides a framework for 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 VANET links [2] [3].

In spite of the ongoing academic and industrial research efforts on VANETs, many research challenges remain. From the network perspective, security is one of the most significant challenges. Vehicle safety applications are among the major drivers for VANETs. Where people's lives are at stake, it is of course essential to secure VANETs against abuse. On the other hand, like all the other wireless networks, a MAC protocol should play a crucial role in scheduling application packet transmissions fairly and efficiently in VANETs, according to the quality of service (QoS) requirements of the applications.

In this paper, we propose a secure MAC protocol for VANETs, with different message priorities for different types of applications to access DSRC channels. The secure communication protocol is designed using time-stamp, digital signature, and trust certificate to guarantee the freshness of the message, message authentication and integrity, message non-repudiation, and privacy and anonymity of the senders.

In the rest of this paper, we first give a brief background on VANETs in Section 2. We present our secure MAC protocol for VANET DSRC applications in Section 3, followed by a detailed simulation and performance analysis in Section 4. Conclusions are given in Section 5.

2. BACKGROUND ON VANETS

2.1. VANET BASICS AND STANDARDS

In a VANET, 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 VANET 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, including Internet access, can be provided to the vehicles. Figure 1 shows an example of a VANET.

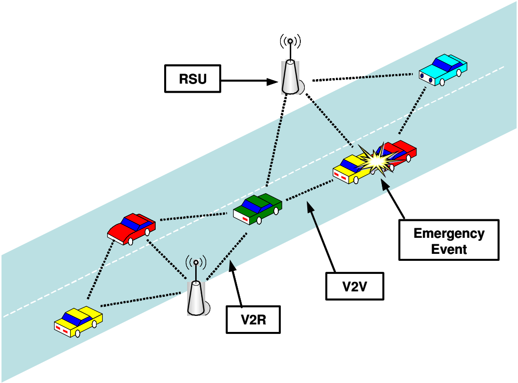


Figure 1. An Example of a VANET

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 [2]. 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.

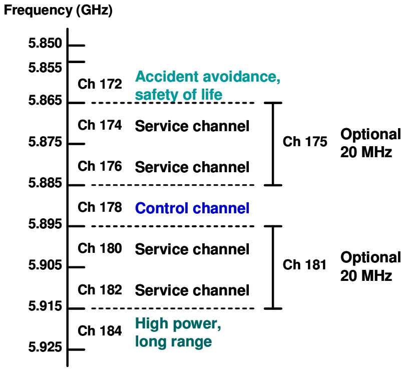


Figure 2. DSRC Channel assignment in North America

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 [4]. 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 [5], 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 ITS 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. VANET APPLICATIONS

In the following we summarize the existing applications and several potential applications that have been proposed for VANETs. As studied in [6] and [7], VANETs would support life-critical safety applications, safety warning applications, electronic toll collection, Internet access, group communications, roadside service finder, etc. In [7] we 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.

Figure 3 lists the characteristics of the example VANET applications discussed in [7], 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.

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

Figure 3. Example VANET Applications

For safety messaging, 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.

2.3. Previous Work on Security in VANETs

In the past few years, considerable effort has been spent in research on VANET networking protocols and applications. However, research on security threats and solutions of VANETs started only recently. While most of the previous studies on VANET security concentrate on particular security mechanisms and solutions on VANET communications (e.g., [7-10]), there are not many works on secure medium access control. In [11] the authors presented a secure MAC protocol for inter-vehicle communication in conjunction with message priority highway safety messaging. The proposed approach uses IEEE 802.11e standard, provides proportional service differentiation in VANET in terms of security, reliability and delay. The work of [11], however, has not considered the DSRC channel structures with the DSRC application scenarios.

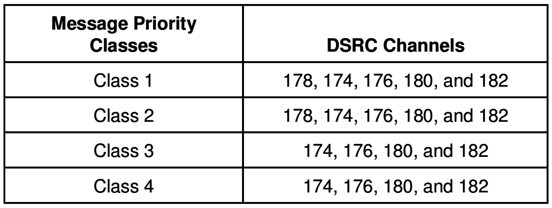
In the WAVE stack, IEEE 802.11p MAC [5] aims at providing the minimum set of specifications required to ensure interoperability between wireless devices attempting to communicate in potentially rapidly changing communication environments and in situations where transactions must be completed in a timeframe, much shorter than that of 802.11 based wireless local area networks (WLAN). The IEEE 1609.2 standard addresses the issues of securing WAVE messages against eavesdropping, spoofing, and other attacks. IEEE 1609.2 security infrastructure is based on industry standards for Public Key Infrastructure (PKI), including the support of Elliptic Curve Cryptography (ECC), WAVE certificate formats, and hybrid encryption methods, in order to provide secure services for WAVE communications. However, IEEE 1609.2 standard does not define vehicle identification and privacy protection, and has left a lot of open issues.

3. A Secure MAC Protocol for DSRC Applications

In this section we propose a secure MAC protocol in consideration of the DSRC channel structures, and to accommodate the DSRC applications while providing adequate security for VANETs. 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 VANETs, and the priority based channel access according to the QoS requirements of the applications.

3.1. Message Priorities of the VANET Communications

As discussed in Section 2.1 from 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. Figure 4 shows the traffic priority classes and the DSRC channels that each class can access.



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

Figure 4. Message Priority Classes and the DSRC Channels

3.2. The Secure Protocol

As it is discussed in [7], VANET 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:

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

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), $Sig_{PrK_V}\{H[M|T]\}$ 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. In (1), the total overhead per packet is 140-Byte with 56-Byte signature and 84-Byte certificate.

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.

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 VANETs: V2R based VANETs, and V2V based VANETs. In V2R based VANETs, 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 V2R based VANETs, on the other hand, we assume there is no RSU infrastructure exist, 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 VANET, unlike in the V2R based VANET where acknowledgement is created by the RSU. Figure 5 and Figure 6 show a V2R based VANET and a V2V based VANET respectively.

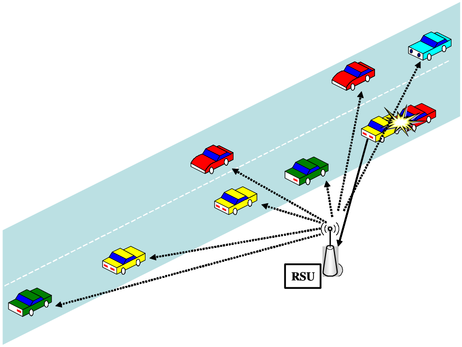


Figure 5. A V2R based VANET

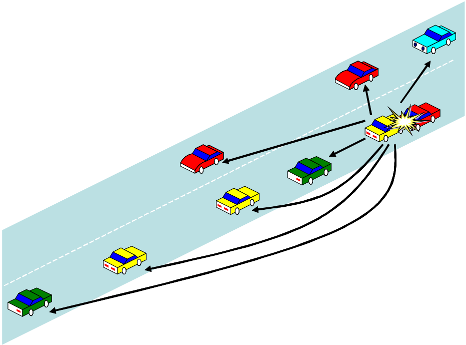


Figure 6. A V2V based VANET

4.1. V2R based VANET Communications

In our simulation, we assume that each vehicle has five interface cards, each of which is operating on a different frequency band. More over, for each channel, we apply the basic parameters of IEEE 802.11. In particular, the main parameters are listed in Table 1 below.

Table 1. Simulation parameters

PARAMETER	VALUE
Basic rate	1 Mb/s
Data rate	1 Mb/s
SIFS	10 us
Slot time	20 us
DIFS	50 us
Size of RTS/CTS/ACK	160/112/112 bits
Size of frame header	224 bits
Size of preamble	48 bits
Minimum window size	31
Maximum window size	1023
Retry limits	5

In addition, we assume that the packet arrival of each class of traffic on every node is exponential with average interval be 100 ms. We also assume that the packet size is fixed to 300 Bytes. Since the packet size is rather small, we use the basic access method instead of the RTS/CTS scheme.

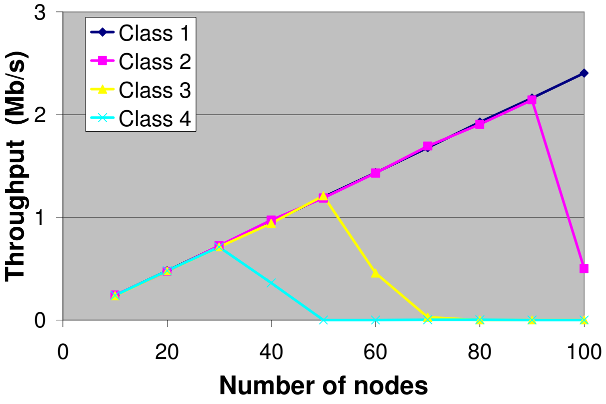


Figure 7. Throughput vs. the number of nodes

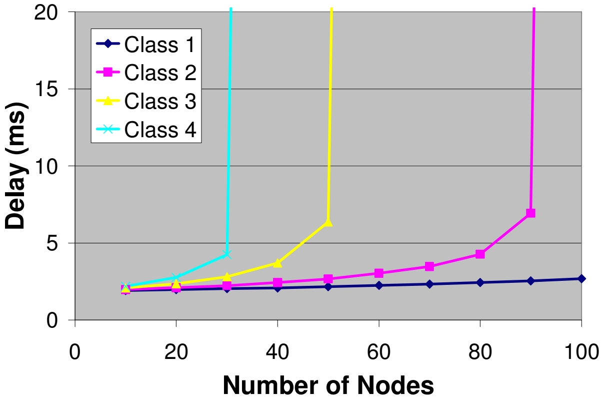


Figure 8. Delay vs. the number of nodes

In Fig.7, we show the throughput performance of the proposed MAC scheme. We can observe that, when the number of nodes in the network is small, all traffic will be accepted and be increased linearly with the increasing of the number of nodes. However, if the number of nodes increases to a certain value, then the performance of lower classes will be decrease, while the throughput of Class 1 can still grow.

Figure 8 illustrates the corresponding delay performance of the proposed scheme. We can see that the average delay for Class 1 traffic is rather stable with the increase of the number of nodes. The other three classes, on the other hand, will be extremely large at certain thresholds.

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 VANETs 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 VANET DSRC applications. Future work is continuing on the performance of V2V based secure communication scenario.

References

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

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

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

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

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

[6] 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.

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

[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.