Secure Vehicular Communication for Safety Applications – A Measurement Study

Juhong Min*, Jihun Ha*, Sangki Yun*, Inhye Kang†, and Hyogon Kim*
*Korea University
†University of Seoul

***Abstract*—In this paper, we explore the feasibility of vehicle-to-vehicle (V2V) secure communication using public key cryptography. We implement a prototype and test it extensively in real driving conditions. Measurement data indicate that the system is feasible in terms of delay and loss, and that we can usually expect better performance than typical simulation works predict. However, we find that traffic congestion and the performance of public key cryptography component can pose significant challenges.**

I. Introduction

The huge success of the IEEE 802.11-based wireless LAN technology has led to its adoption in the Intelligent Transportation Systems (ITS) for safety enhancement, among others. For instance, the Dedicated Short Range Communications (DSRC) [1] for North American cars and trucks in the 5.9 GHz band is envisioned to enable roadside safety, as well as traffic information and entertainment services. The standardization of physical (PHY) and multiple access control (MAC) layer protocol is ongoing in the IEEE 802.11p working group [2], based on 802.11 MAC and 802.11a PHY standards.

Arguably the most critical issue in deploying wireless technology in ITS safety applications is security. As malicious interference with the communication of safety information between vehicles (*e.g.*, imminent collision warning) can have catastrophic consequences, it is highly desirable that the safety information is protected by accompanying security protocol. In this paper, therefore, we consider a light-weight public key cryptography system for vehicle-to-vehicle (V2V) communication environment, and evaluate its feasibility through real-life roadside performance measurements.

Specifically, we collect the encryption–decryption delay of the on-board public key cryptography system as well as the wireless delay and loss data in the real V2V communication using 802.11 devices in various roadside environments. Then we assess the collected data in the light of the safety requirements in the high-speed driving environment.

The findings of this study can be summarized as follows:

- Delay and loss performance is significantly better up to a large distance than what is typically assumed in existing simulation models. As a consequence, the value of multi-hop relaying of messages is considered dubious.
- Inter-vehicle distance and velocity is not as much a problem as traffic congestion. The loss characteristics of the transmission under congestion degrades fast even within a short distance.
- In contrast to prior works that predict the 802.11 MAC performance degradation in case of repetitive message transmissions, our study reveals that the public key cryptography component can become the bottleneck rather than the MAC.
- All in all, the performance of secure communication using the public key cryptography and the IEEE 802.11 technology in V2V environment is acceptable within the critical distance where the loss or excessive delay of the safety information can have the most dire consequences.

We elaborate on these observations below.

II. A V2V secure communication architecture

In this section, we illustrate a light-weight public key cryptograph architecture that can be used for secure communication in V2V environments. However, we remark here that it is not the central theme of this paper to predict the exact manifestation of the secure communication architecture in V2V environments. Rather, it is how such a system with a public key cryptography component fare in real roadside V2V communication situation.

A. Why public key cryptography

We assume that the vehicles that happen to exchange urgent safety information do not know each other *a priori*. This naturally disqualifies the use of a prescribed symmetric key, since it would require the secret (*i.e.*, the symmetric key) sharing across vehicles to be too wide, making the compromise of the symmetric key easier for attackers and the impact of the breach far-reaching.

The use of pairwise session keys spontaneously set up between the vehicles is also out of the question, in light of the timing requirement for safety information exchange. This is especially true because the safety information should be broadcast to all vehicles in the area of critical event. A group session key set up between all involved parties that can be unpredictably large and highly fluctuating in number would also take too long a time. For instance, 200ms is the widely accepted limit for the communication delay [3], and it would be extremely difficult to negotiate the group key and then exchange the critical safety information before the safety event unfolds. Therefore, in this paper we assume that the V2V secure communication should rely on public key cryptography. Although the public key cryptography is known to be slow, it is not expected to cause a severe problem for short messages typically used in the safety applications [4].

978-1-4244-1645-5/08/$25.00

B. A secure V2V communication architecture

In our scheme, a vehicle A is issued a certificate $\{P_A\}_{V_C}$, which is signed by the certification authority (CA) C, where P_A and V_C are the public key of A and private key of C, respectively. The certificate should be preloaded, *e.g.*, during the manufacturing of the vehicle. Also, we assume that each vehicle is equipped with a GPS device, with which the secure communication system has an interface. It is not an unreasonable assumption since such applications as Cooperative Collision Warning (CCW) require GPS devices with fine resolution in order to properly associate vehicles with lanes or to compute relative positions [4].

When A needs to transmit a safety message, it broadcasts a 3-tuple $\{\{T_{GPS},\ M\}_{V_A},\ \{P_A\}_{V_C},\ C\}$, where M is the message and T_{GPS} is the GPS time at the time of transmission. The timestamp is necessary to prevent playback attack. Without the timestamp, an attacker can pick up a transmission $\{\{M\}_{V_A},\ \{P_A\}_{V_C},\ C\}$, and replay it whenever and wherever it wants because a receiver cannot check how "fresh" the information is.[1] If M is an urgent message such as Electronic Emergency Brake Light (EEBL) or Forward Collision Warning (FCW) [4] that requires a quick responsive action from the receivers of the replayed message (*i.e.*, vehicles that happen to be near the attacker), they can be confused and fall into a dangerous situation.

Once a receiver B gets the encrypted message, it first looks up C in the list of its trusted CA's for P_C. If C is found, it uses P_C, to recover P_A. Now, B can decrypt M and obtain T_{GPS}. It then compares T_{GPS} with its own GPS time t. If $(t - T_{GPS}) < \delta$, where δ is the freshness threshold, B takes the message as not replayed, and conveys M to the driver. The specific value of δ can be arbitrarily small, *e.g.* 1 second, as long as it can prevent the replay attack. Fig. 1 shows the message decryption process.

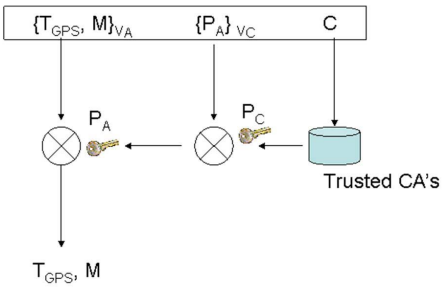

Fig. 1. Message decryption process at the receiver

The encrypted message is broadcast to an indefinite number of neighboring vehicles. The IEEE 802.11 broadcast does not provide MAC level acknowledgement, so the delivery is not guaranteed. Therefore, the safety application must take account of the possibility of communication failure, for instance in case of bad channel or severe MAC level collisions. We assume that each vehicle broadcasts the same message multiple times as in [9].

[1]We can also include the GPS position data in the transmission, but it is not used in our implementation to reduce the message size and because of the dependency between the time and location of the message transmission.

C. Laboratory test

We implemented and tested the public key cryptography software based on a publicly available elliptic curve cryptograph (ECC) algorithm implementation with 112-bit key size [5] in the laboratory setting, where two laptops running the code were put in close proximity with line of sight (LOS). We measured the secure wireless communication delays over 1,000 transmissions. The sum of the application processing (message generation, encoding and decoding) plus the UDP/IP/802.11g communication delays in the environment was centered around 52±1ms (Fig. 2). This is considered the lower bound of the communication delay of the implemented system. In contrast, the plaintext transmission of the same message takes less than 3ms for vast majority of the frames (not shown for space). So the encryption–decryption delay is significant.

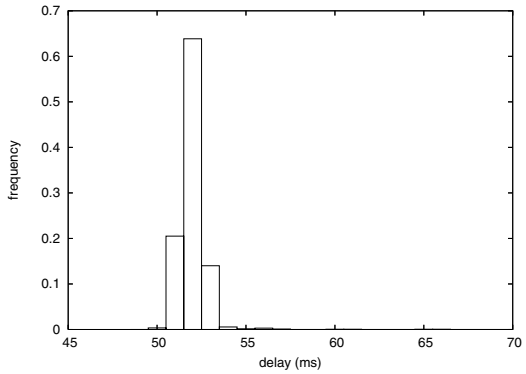

Fig. 2. Delay measured in laboratory environment

III. Data collection

For data collection, in total we drove approximately 1,500km and collected 53,000 data points while shuttling two cars between Seoul and Munsan city, 47km from Seoul (Fig. 3). The data collection was done on a regional highway called the Freedom Expressway connecting the World Cup Stadium in Seoul and Munsan City along the Han River. This road was chosen because it was relatively detached from the residential areas where the 802.11 b/g APs are now widely used. As our WLAN cards simulate 802.11p on-board units that will not be interfered by the residential 802.11 b/g devices, we needed to conduct the experiments off the residential areas.

We used two Fujitsu laptop computers running Linux Fedora Core 6, equipped with Proxim Orinoco 802.11b/g Gold WLAN card. They were supplemented by an omni-directional external antenna for a 6dB gain, which was mounted on top of the car (Fig. 4). These laptops communicate while they are each carried in a car, whose velocity and the distance from each other is recorded every second by the Garmin legend Cx GPS receiver. After the data collection, we matched the GPS log with the measurements from the laptops.

Every second, 200 packets were transmitted by one of the laptops, carrying the identical message $\{\{T_{GPS},\ M\}_{V_A},\ \{P_A\}_{V_C},\ C\}$, which is 313 bytes in size. No RTS/CTS was used, and we fixed the nominal

Fig. 3. Driving map from Seoul to Munsan (Source: Google Earth^{TM}).

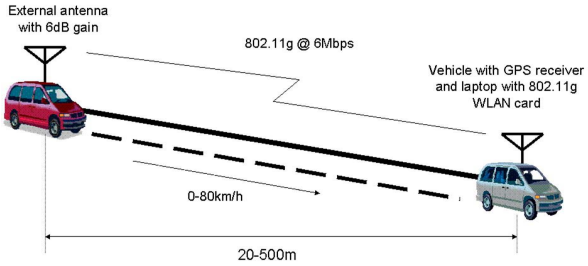

Fig. 4. Summary of the experiment setup.

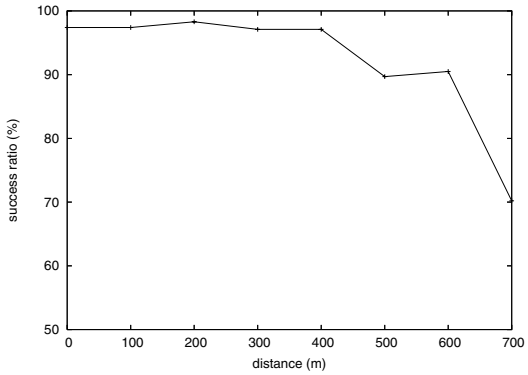

Fig. 5. Impact of inter-vehicle distance on delivery success ratio

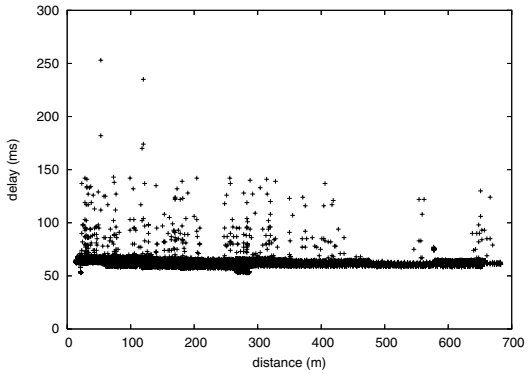

Fig. 6. Impact of inter-vehicle distance on delay

transmission rate to 11Mbps, a basic rate in the 802.11g, as the main mode of transmission in the safety application will be broadcast and MAC layer broadcast uses a basic rate.

In the measurement, what we focus on are the delay and the successful delivery ratio (*i.e.*, 1− loss ratio) of the safety information frame. Unlike some prior works, we are less interested in the long-term TCP or UDP throughput [6], because the size of the safety information exchanged between vehicles in driving situation should be typically small.

IV. Analysis

A. Inter-vehicle distance

In the first experiment, we measure the impact of the distance between the two vehicles on the delay and the delivery success ratio. We maintained the speed of the experiment vehicles at 70km/h (or 43mi/h), varying the distance in between. The road condition at the time of measurement was slightly loaded at 2,183 vehicles per hour, with average speed of 85.2km/h (53mi/h) [7].

Fig. 5 shows the delivery success ratio as a function of the inter-vehicle distance. We notice that within 400m distance, the broadcast transmission suffers only minor losses, *i.e.*, within 3%. This loss performance is far better than what is assumed in some prior simulation works [4], [8]. For other road conditions below, the loss characteristics is also consistently better. It is a good news for the DSRC safety applications. For instance, the entire highway chain crash episode is modeled within much less than 400m radius in [8].

Fig. 6 shows the delay distribution of the successfully delivered frames of Fig. 5. We observe that most frames were received within 150ms (the postmortem analysis revealed that the occasional large delays were caused by OS-internal bookkeeping), where the vast majority center around 60ms. Interestingly, the delay does not change with increasing distance, implying that propagation delay is a marginal factor. Compared with the laboratory measured delay values (Fig. 2), this experiment shows, the delay only slightly increases in real driving situation.

In summary, in the highway environment, the distance between communicating vehicles is not likely the critical factor for loss and delay performance of the public cryptography communication. Up to 400m the communication has 97% delivery success ratio, and up to 600m, 89%. This result implies that a few duplicate transmissions will effectively eliminate the possibility of message loss. For instance, 3 and 5 transmissions within 400m range will lower the loss probability to 10^{-5} and 10^{-8}, respectively. Finally, the transmission range with low loss and delay is sufficiently large for safety application perspective, so multi-hop message relay of urgent safety information seems not necessary.

B. Vehicle speed

Based on the observation that the inter-vehicle distance is not critical up to 400m or so, here we fix it to 50m and measure the same metrics while varying the speed from 5 to 140km/h. At the time and locale of the measurement, the traffic volume was 727 vehicles per hour [7], only one third of that from the first experiment. With the reduced distance between the vehicles, the delivery success ratio was consistently near 97%, irrespective of the speed (not shown for space). Fig. 7 shows the delay distribution for the given range of vehicle speeds.

We do not notice any significant deviation from Fig. 6. All in

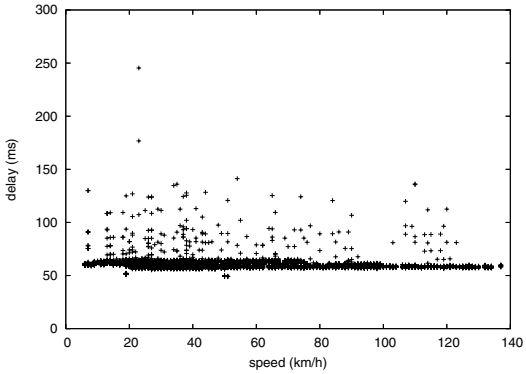

Fig. 7. Impact of vehicle speed on delay

all, the realistic driving speed (*i.e.*, $<$ 140km/h) does not affect the delay and loss performance of the secure communication.

C. Traffic congestion

Vehicle traffic congestion could adversely affect the V2V communication. In this experiment, we performed the measurement experiment in three different driving environments in terms of congestion, which are compared in Table I. The Congested environment refers to the driving condition within the center city Seoul at rush hour. The traffic moves slowly, and the traffic volume is high. The Urban environment is driving from the city edge towards the center city. The traffic volume and speed are both better than in the Congested environment. The Rural environment corresponds to driving outside Seoul in a sparsely populated area. In all three environments, we followed the traffic naturally without consciously controlling the vehicle speed or the inter-vehicle distance. The measured data shows that the speed in all three was under 50km/h, and the distance between the experiment vehicles was below 150m.

TABLE I
3 DRIVING ENVIRONMENTS

Environment	**Traffic condition**	
	Avg. speed (km/h)	Traffic vol. (/h)
Congested	12.5	1,021
Urban	46.2	252
Rural	*Very light*	

Fig. 8 shows the delivery success ratio as a function of the vehicle distance in the three environments. We notice that the loss rate visibly increases with traffic congestion. For instance, the loss rate is close to 30% in the Congested environment, even for 150m distance. This is in contrast to Fig. 5, where the loss rate is consistently less than 3% within 400m range. We suspect that the increased reflection against metal hulls of ambient cars and the loss of LOS between the two experiment vehicles due to heavy traffic contributed to the increase of multipath fading hence high loss rates.

The exact analysis of the loss rate increase is still to be done, but the implication is clear. Unlike the distance or the speed of the communicating vehicles, the traffic congestion

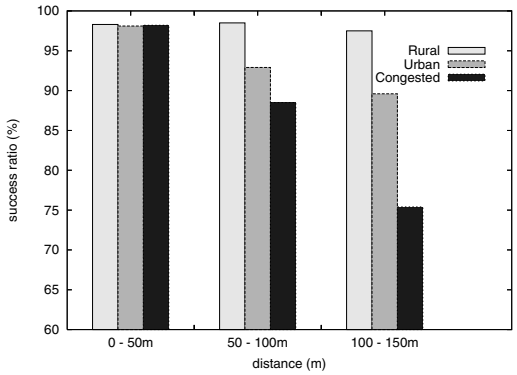

Fig. 8. Impact of traffic congestion on loss

can significantly affect the frame delivery even within a relatively short distance. A straightforward solution approach would be to increase the number of duplicate transmissions to improve the delivery ratio [9]. With 3 transmissions, the loss probability can be reduced to 10^{-2}, and 5 retransmissions, 10^{-3}. However, if vehicles independently take this approach in a congested area, the 802.11 MAC collision problem will be aggravated [9]. A further examination of the interaction between the two sources of frame losses is necessary, which will be done in our future work.

The delay distribution for the successfully received frames is not different from those of the previous experiments. In particular, the three different environments do not show any noticeable correlation with the delay data. The delays from all three environments are indistinguishable. Fig. 9 shows the measurement result.

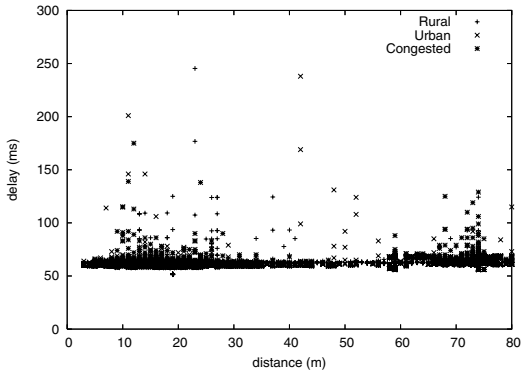

Fig. 9. Impact of traffic congestion on delay

D. Message flooding

As wireless broadcast channel is inherently unreliable, the repetitive transmission of the same message is essential. However, the cost is the increased traffic load, even leading to the MAC layer message losses [9]. In this experiment, we explore the impact of message flooding on the secure communication performance. This could happen if multiple cars broadcast (duplicated) safety related messages in proximity. We let multiple wireless stations transmit the encrypted safety message whose format is as defined in Section II-B, and observe the impact of the increased number of transmitters. Specifically, we let multiple transmitters send 50 encrypted message at 100ms interval, and how a single receiver copes with the flooding.

We perform this experiment in the laboratory environment, so the wireless stations are located in close proximity and with LOS. The possibility of frame loss due to adverse channel condition is thus low, and the frame loss is all due to collision. In Fig. 10, we show the delay distribution of the messages. In the figure, `1:4` and `1:5` means the original system that

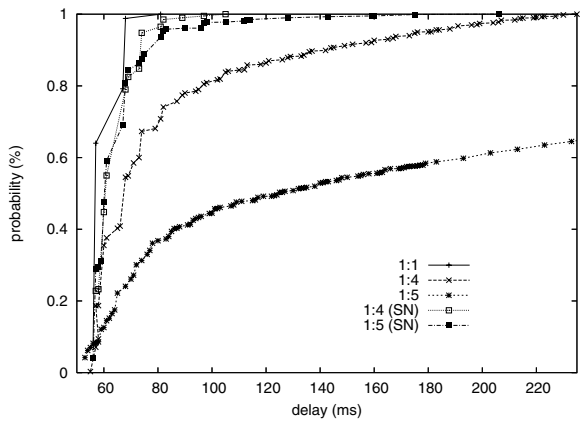

Fig. 10. Impact of message flooding on delay

we proposed in Section II-B, with 4 and 5 broadcasters, respectively. We observe that for such system, the flooding has a devastating effect. The reason that the delay soars is the decryption[2]. Through the inspection of the system log, we found that the message queue to the decryption routine grows unbounded under such heavy load. Assuming that the public domain ECC implementation we used [5] is reasonably optimized, it reveals a new aspect of secure communication performance in public key cryptography. Message flooding has been a concern in terms of the 802.11 MAC performance [9], but our prototype implementation of the ECC shows that the decryption can become a bottleneck well before the MAC is overloaded.[3]

As a partial solution to this problem, we included a serial number (SN) for the messages, where duplicate ones share the same SN. So the modified message format is $\{\{T_{GPS},\ M\}_{V_A},\ \{P_A\}_{V_C},\ C,\ SN\}$. When the receiver receives multiple copies of the duplicate message, it drops all except the first arriving one. It saves the effort to decrypt the discarded messages. In Fig. 10, `1:4(SN)` or `1:5(SN)` means the delay performance after applying this modification. The result shows that the serial number scheme effectively filters the unnecessary processing of the duplicate messages, and the performance penalty is now marginal compared to the single broadcaster case (`1:1`).

E. Application to chain crash model

In Fig. 7, we noticed that the vast majority of the delays between two vehicles in highway driving situation lie within 150ms. Using the chain crash model of [8] and this data, here we compute how the secure communication helps reduce the extent of chain crash. In the original scenario, 5 vehicles cruise at 73mi/h (32m/s), the inter-car spacing is 32m (1s), the driver reaction time is assume to be 1.5s, and the deceleration is 4m/s^2. The first car breaks at 160m and stops at 280m, and the following 4 cars need to stop before collision. In this original scenario without wireless communication, all 5 cars chain crash. But under the secure communication with 150ms of message delivery delay, we see in Fig. 11 that only 2 cars are involved in the crash event.

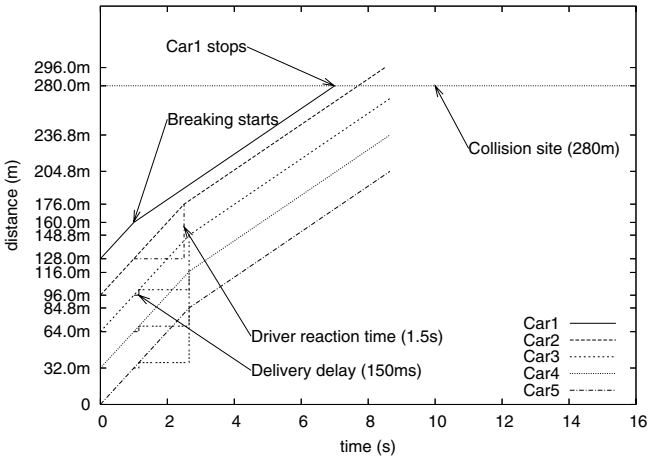

Fig. 11. Chain crash scenario

V. Future work

Through extensive roadside measurements in this study, we found that encrypted wireless communication over the IEEE 802.11 channel can be effective in terms of delay and loss for safety applications, over a significant distance. But we also found that traffic congestion and the performance of the public key cryptography component can pose challenges. In our future work, we plan to investigate these issues further. Also, the effect of adverse weather condition on the communication performance will be explored, since the weather condition is directly related with the roadside safety aspects.

[2]Note that we exclusively use 802.11 broadcast that does not use retransmission, so the measured delay does not contain retransmission delay.

[3]Non-ECC public key cryptography such as RSA or Diffie-Hellman can aggravate the problem since the ECC method is generally faster.

References

[1] "What is DSRC?" http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[2] IEEE P802.11 - TASK GROUP P, "Status of Project IEEE 802.11p," http://grouper.ieee.org/groups/802/11/Reports/tgp_update.htm.

[3] Q. Xu, R. Sengupta, and D. Jiang, "Design and Analysis of Highway Safety Communication Protocol in 5.9 GHz Dedicated Short-Range Communication Spectrum," Proc. IEEE VTC, vol. 57, no. 4, 2003, pp. 2451–55.

[4] Tamer ElBatt, Siddhartha Goel, Gavin Holland, Hariharan Krishnan, Jayendra Parikh, "Cooperative Collision Warning Using Dedicated Short Range Wireless Communications," In Proc. ACM VANET, 2006.

[5] Crypto++ Library 5.4, *Crypto++ : open source crypto package written in C++ with ECC library*, Available at http://www.cryptopp.com.

[6] Ott, J. and Kutscher, D., "Drive-thru Internet: IEEE 802.11b for "Automobile" Users." in Proc. IEEE INFOCOM 2004.

[7] Seoul metropolitan area real-time traffic volume data. Available at http://www.spatic.go.kr.

[8] S. Biswas, R. Tatchikou and F. Dion, "Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety," *IEEE Communications Magazine*, vol.1, pp. 74-87, 2006.

[9] Qing Xu, Tony Mak, Jeff Ko, Raja Sengupta, "Vehicle-to-vehicle safety messaging in DSRC," In Proc. ACM VANET, pages 19-28, 2004.