

# Accelerating Authenticated Emergence Message Propagation to Mitigate Chain-Reaction Accidents in Highway Traffic

Rongxing Lu<sup>†</sup>, Xiaodong Lin<sup>‡</sup>, Haojin Zhu<sup>§</sup>, and Xuemin (Sherman) Shen<sup>†</sup>

<sup>†</sup>Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

<sup>‡</sup>Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, Ontario, Canada

<sup>§</sup>Department of Computer Science and Engineering, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai, China  
Email: {rxlu, xshen}@bcr.uwaterloo.ca; Xiaodong.Lin@uoit.ca; zhu-hj@cs.sjtu.edu.cn

**Abstract**—The chain-reaction collision caused by a sudden event such as deer-vehicle collision is a serious accident in highway traffic. By propagating the authenticated emergence message on deer-vehicle collision with vehicle-to-vehicle (V2V) communication, the chain-reaction accident could be mitigated. However, the long delay imposed by traditional signature based authentication may weaken the effectiveness of such message propagation. In this paper, in order to accelerate the propagation, we propose a new online/offline Rabin signature scheme integrated in an authenticated emergence message propagation model. With the proposed signature scheme, the emergence message can be quickly signed and verified, and thus the propagation is accelerated. Extensive simulation results also demonstrate the effectiveness of the proposed scheme.

**Keywords**— Deer-vehicle collision, chain-reaction accident, on-line/offline Rabin signature, propagation model

## I. INTRODUCTION

With the increase of deer population and traffic patterns in North America, deer-vehicle collisions have become a major problem in highway traffic. Every year the deer-vehicle collisions take a huge toll in lives, money and time [1], [2]. By statistics, in 1995, an estimated 726,000 deer-vehicle accidents resulted in \$1.2 billion in damages. In 1998, an estimated 13,500 deer-vehicle collisions in Iowa alone resulted in more than \$10 million in personal injury and property damage [1]. In the early years of the 21st century, there is still an estimated 1,500,000 deer-vehicle collisions occurring annually [2].

The above statistics is shocking. However, the huge toll doesn't merely rise from the deer-vehicle collision, but from the subsequent chain-reaction collision, as shown in Fig. 1. The chain-reaction collision is a serious traffic accident in highway, which usually involves multiple vehicles and the vehicle behind will collide with the front vehicle to cause large damage. For example, it was reported in October 2008 that, when a minivan collided with an elk on the stretch of Highway 2 south of Calgary, a four-vehicle chain-reaction collision took place and caused 11 people injured. From this realistic observation, if the subsequent chain-reaction collision can be avoided, the loss due to a sudden deer-vehicle collision will be reduced. The major cause of a chain-reaction collision is that drivers close to a sudden car accident scene don't

have enough time to react due to many facts, such as poor visibilities, following too close. Obviously, the chain-reaction collision can be avoided if the drivers approaching the scene are alerted as earlier as possible when the collision happens.

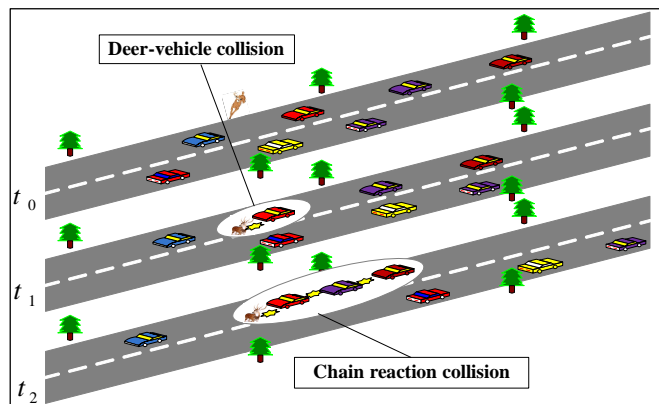


Fig. 1. A typical vehicle chain-reaction collision caused by a sudden deer-vehicle collision in highway traffic environments.

Recent advance of wireless communication technologies have given rise to a promising approach for improving road safety and efficiency through vehicle-to-vehicle (V2V) communication [3]–[6]. For instance, many major car manufacturers and telecommunication industries have recently geared up to equip each car with the wireless technology that allows different car to communicate with each other to not only improve road safety but also the driving experience. Therefore, to avoid/mitigate the chain-reaction collisions, a potential solution can be provided by V2V communication [7]–[9], in which the emergence message on a deer-vehicle collision can be quickly propagated to other approaching vehicles. Nevertheless, when an emergence message is propagated by V2V communication, it must be authenticated [4], [5]. Otherwise, a malicious vehicle may propagate a bogus message to destroy the road safety.

To authenticate the emergence message, currently there exist two potential solutions. One is by the efficient message authentication code (MAC) [10]. However, this technique may not be

applicable in V2V communication since it requires the source of emergence message shares keys with all its neighboring vehicles. Another solution is by digital signature technique [10], so anyone can check the validity of the emergence message. However, it can be observed that the traditional digital signature schemes (including online/offline schemes) are not efficient in either signing phase or verification phase. Thus, a long authentication delay on emergence message is inevitable, which results in the failure of mitigating the chain-reaction collision in highway.

Therefore, it is crucial to successfully utilize V2V communication to reduce chain-reaction collision by having an efficient digital signature scheme. To address the delay issues lying in authenticated emergence message propagation, in this paper, we propose a new online/offline Rabin signature scheme. Compared with the previously reported schemes [10], the proposed scheme is more efficient. Thus, it can accelerate the propagation of the authenticated emergence message on deer-vehicle collision.

Concretely, the contributions of this paper are threefold.

- First, we propose an efficient online/offline Rabin signature scheme based on factoring problem. To the best of our knowledge, this is the *first* efficient online/offline signature in both signing phase and verification phase.
- Second, we model a simple emergence message propagation in highway traffic. Within this model, we quantitatively analyze the effectiveness of the proposed scheme.
- Third, we develop a Java simulator to show the substantial improvement of authenticated emergence message propagation under the proposed online/offline signature scheme. The experimental results show that the emergence message propagation under the proposed online/offline signature is more efficient than that others.

The remainder of this paper is organized as follows. We first formalize the problem in Section II, and then describe the related work in Section III. The proposed online/offline Rabin signature is presented in Section IV. Section V introduces the proposed propagation model, followed by the performance evaluation in Section VI. Finally, conclusion remarks are given in Section VII.

## II. PROBLEM FORMALIZATION

In this section, we provide a concise problem formalization, including system model and design goals.

### A. System Model

By long-term observations and statistics, vehicles running in the highway usually form different clusters in an *ad hoc* pattern. For example, those vehicles with same direction, same velocity, and same lane can form a temporal cluster, and this cluster is dynamic but relatively steady during a certain period. Therefore, in our system model, we consider there are many temporal vehicle-clusters scattering in the highway traffic environments, as shown in Fig. 2. Since different vehicle-clusters are not adjacent to each other in the same lane, (otherwise they will be merged as one cluster), a chain-reaction

collision taking place in one cluster won't affect other clusters. Therefore, we restrict our work to a single vehicular cluster moving over a single lane in highway traffic.

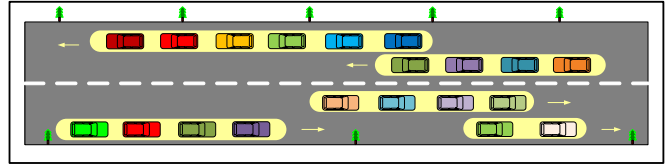


Fig. 2. System model under consideration.

Let  $\mathcal{VC}$  be a vehicle-cluster which consists of  $N$  vehicles  $\{V_1, V_2, \dots, V_N\}$ . Each vehicle  $V_i \in \mathcal{VC}$  is equipped with a uniquely identified transmitting device, called onboard-unit (OBU), to communicate with other vehicles within its transmission range. All vehicles in  $\mathcal{VC}$  form a long vehicle queue moving in a single lane. Assume that the length of each vehicle is  $l$ , and the average distance between two vehicles is  $L$ . For highway environments, it is naturally believed that  $l \ll L$ . Then, the length of the whole queue is approximately  $L \cdot (N - 1)$ . Assume that the transmission range of each vehicle is  $R$ . If  $R \geq L \cdot (N - 1)$ , the emergence message propagation about a sudden deer-vehicle collision only requires one hop. However, when  $R < L \cdot (N - 1)$ , the emergence messages have to be propagated via more than one hop, which will lead a long propagation delay  $T_D$  of a surety. In addition, when a vehicle transmits an emergence message within a vehicle cluster, the success transmission probability of the sender is  $p$ , ( $0 < p < 1$ ). Note that this channel model, although very simple, can capture the uncertainty about correct emergency message propagation.

### B. Design Goals

To avoid a chain-reaction collision in highway traffic, each vehicle in the same  $\mathcal{VC}$  is eager to receive an authenticated emergence message as quick as possible. Therefore, it is of ultimate importance to accelerate the authenticated emergence message propagation in the vehicle cluster  $\mathcal{VC}$ , which hereby will be addressed in this paper. Specifically, we design a novel efficient online/offline Rabin signature scheme. By modelling the exact authenticated emergence message propagation in highway traffic, we demonstrate the efficiency of the proposed online/offline signature scheme, i.e., the proposed scheme can reduce the delay to mitigate the vehicle chain-reaction collision.

## III. RELATED WORK

### A. Multi-Hop Emergency Message Propagation

Recently, much research work [7]–[9] has explored how to avoid/mitigate traffic accident and injuries with multi-hop emergence message propagation in VANET. In [7], Resta et al. analyze the dynamics of multi-hop emergency message dissemination in VANETs. Under a probabilistic wireless channel model that accounts for interference, the authors derive lower bounds on the probability that a vehicle at distance  $d$  from

the source of the emergency message correctly receives the message within time  $t$ . In [8], Oh et al. present location-aware protocols for delivering emergency warning messages with improved reliability to nearby and approaching vehicles. In [9], Tsai and Du also propose an aggressive access strategy to delivery emergence message to prevent accident in advance.

Although the above schemes are novel, the propagation security hasn't been addressed. In other words, the emergency messages haven't been authenticated, and the bogus messages could be mingled.

### B. Online/Offline Signature

The notion of online/offline signature was first introduced by Even et al. in [11]. The main idea of the online/offline signature is to perform the signature generation procedure in two phases. The first phase is executed offline (which is irrelevant to the message to be signed) and the second phase is performed online (after the message to be signed is given). Since the online/offline signature can add costly computations executed in offline phase, the online phase is typically very fast. Therefore, online/offline signature scheme is very useful in many applications where the signer has a very limited time once the message is presented. Some discrete logarithm (DL) based signature schemes, such as Schnorr, El-Gamal, and DSS [10], are online/offline signature schemes in nature, since the costly computations in these schemes do not depend on the given messages and can be carried out offline. However, not all signature schemes have such a characteristic. Thus, Even et al. [11] presented a general method to convert any signature scheme into an online/offline signature scheme, but it is not efficient and practical. In 2001, based on the trapdoor hash function, Shamir and Tauman [12] proposed another generic method to achieve online/offline signing. Although the online signing phase becomes very fast, the verification phase in these online/offline schemes still requires costly computation. As a consequence, if the computation costs in verification phase can't be improved, these existing online/offline schemes are not particularly suitable for accelerating authenticated emergence message propagation.

Rabin signature [13] and its improved version [14] are very efficient in signature verification, since only one modular square operation is required. However, the signing phase of Rabin signature is comparably slow. Therefore, it is worth accelerating the speed of signing phase. Aiming at this goal, we will propose a new online/offline Rabin signature scheme in the next section, which is efficient in both signing and verification phases.

## IV. PROPOSED EFFICIENT ONLINE/OFFLINE RABIN SIGNATURE

In this section, we present a new efficient online/offline Rabin signature scheme, which includes system setup, signing algorithm and verification algorithm. The main idea of the proposed scheme is to reduce the computation costs in both online signing phase and verification phase as short as possible

so that it can be used to accelerate authenticated emergence message propagation.

**System setup:** Given a security parameter  $\lambda$ , two  $\lambda$ -bit safe primes  $p$  and  $q$  are firstly chosen, where  $p \equiv q \equiv 3 \pmod{4}$ . Compute the module  $n = pq$ ; choose two random numbers  $x_1, x_2 \in \mathbb{Z}_n^*$ , and compute  $y_1 = x_1^2 \pmod{n}$ ,  $y_2 = x_2^2 \pmod{n}$ . Choose a random number  $a \in \mathbb{Z}_n^*$  satisfying the Jacobi symbol  $\left(\frac{a}{n}\right) = -1$ . In addition, a secure hash function  $H : \{0,1\}^* \rightarrow \mathbb{Z}_n^*$  will be chosen as well. Then, the public key  $pk$  is  $(n, y_1, y_2, a, H)$  and the private key  $sk$  is  $(p, q, x_1, x_2, x_2^{-1} \pmod{n})$ .

### Signing Algorithm:

- **Offline Phase:** In idle time, the signer, with the private key  $sk$ , executes the following steps:

- 1) choose a random number  $b \in \mathbb{Z}_n^*$  and compute

$$B = b^2 \pmod{n} \quad (1)$$

- 2) compute the hash value  $H(B)$  and the bit  $c_1$ , where

$$c_1 = \begin{cases} 0, & \text{if } \left(\frac{H(B)}{n}\right) = 1 \\ 1, & \text{else if } \left(\frac{H(B)}{n}\right) = -1 \end{cases} \quad (2)$$

- 3) compute  $B' = a^{c_1} \cdot H(B)$  and the bit  $c_2$ , where

$$c_2 = \begin{cases} 0, & \text{if the Legendre symbol} \\ & \left(\frac{B'}{p}\right) = \left(\frac{B'}{q}\right) = 1 \\ 1, & \text{else if } \left(\frac{B'}{p}\right) = \left(\frac{B'}{q}\right) = -1 \end{cases} \quad (3)$$

- 4) compute  $B^* = (-1)^{c_2} \cdot a^{c_1} \cdot H(B) \pmod{n}$ ; apply the Chinese Remainder Theorem to compute one root  $s^*$  of the congruence  $s^2 \equiv B^* \pmod{n}$  such that  $\left(\frac{s^*}{p}\right) = \left(\frac{s^*}{q}\right) = 1$ .
- 5) store the entry  $(b, c_1, c_2, s^*)$  in a pool; after this, if the signer is still in idle, s/he goes back to step 1.

- **Online Phase:** For a message  $m \in \mathbb{Z}_n^*$ , the signer chooses an unused entry  $(b, c_1, c_2, s^*)$  from the pool and runs the following steps:

- 1) compute a random number  $r$  from the relation  $x_1 \cdot m + x_2 \cdot r = b \pmod{n}$ , where

$$r = (b - x_1 \cdot m) \cdot x_2^{-1} \pmod{n} \quad (4)$$

- 2) since

$$\begin{aligned} x_1 \cdot m + x_2 \cdot r &= b \pmod{n} \\ \Rightarrow (x_1 \cdot m + x_2 \cdot r)^2 &= b^2 = B \pmod{n} \\ \Rightarrow y_1 \cdot m^2 + m \cdot 2 \cdot x_1 \cdot x_2 \cdot r + y_2 \cdot r^2 &= B \pmod{n} \end{aligned} \quad (5)$$

the signer sets

$$a_1 = x_1 \cdot x_2 \cdot r \pmod{n}; \quad a_2 = r^2 \pmod{n} \quad (6)$$

- 3) In the end, the signature  $\sigma$  on the message  $m$  is  $(a_1, a_2, c_1, c_2, s^*)$ .

**Verification Algorithm:** For a signature  $\sigma = (a_1, a_2, c_1, c_2, s^*)$  on the message  $m$ , any verifier can first compute

$$B = y_1 \cdot m^2 + m \cdot 2 \cdot a_1 + y_2 \cdot a_2 \bmod n \quad (7)$$

and verify the signature by checking the following equations

$$\begin{cases} s^{*2} \stackrel{?}{\equiv} (-1)^{c_2} \cdot a^{c_1} \cdot H(B) \bmod n \\ a_1^2 \stackrel{?}{\equiv} y_1 \cdot y_2 \cdot a_2 \bmod n \end{cases} \quad (8)$$

If both of them hold, the signature  $\sigma$  can be accepted, otherwise rejected.

**Efficiency:** In the proposed online/offline Rabin signature scheme, the online phase only requires 4 modular multiplications (Mu) and 1 modular square (Sq), and the verification algorithm also only requires  $6 \cdot \text{Mu} + 3 \cdot \text{Sq}$ . Therefore, compared with other online/offline signature schemes [12], this scheme is more efficient in terms of computation costs.

**Security:** The proposed online/offline Rabin scheme is not only efficient but also secure against existential forgery attack. On one hand,  $(B, c_1, c_2, s^*)$  is provably secure in the random oracle model [15]. On the other hand,  $(a_1, a_2)$  is also protected by the quadratic root problem. Suppose an adversary  $\mathcal{A}$  holds a valid signature  $(a_1, a_2, c_1, c_2, s^*)$  on message  $m$ , he wants to forge another valid signature  $(\tilde{a}_1, \tilde{a}_2, c_1, c_2, s^*)$  on a new message  $\tilde{m}$ . Then, the challenge confronting with him is to solve  $(\tilde{a}_1, \tilde{a}_2)$  from

$$\begin{cases} y_1 \cdot \tilde{m}^2 + 2 \cdot \tilde{m} \cdot \tilde{a}_1 + y_2 \cdot \tilde{a}_2 = B \bmod n \\ \tilde{a}_1^2 = y_1 \cdot y_2 \cdot \tilde{a}_2 \bmod n \end{cases} \quad (9)$$

Based on Eq. (9), we have

$$y_1 \cdot \tilde{m}^2 + 2 \cdot \tilde{m} \cdot \tilde{a}_1 + \tilde{a}_1^2 \cdot y_1^{-1} = B \bmod n \quad (10)$$

Let  $A = y_1^{-1}$ ,  $B = 2 \cdot \tilde{m}$ , and  $C = y_1 \cdot \tilde{m}^2 - B$ , then Eq. (10) is converted as

$$A \cdot \tilde{a}_1^2 + B \cdot \tilde{a}_1 + C = 0 \bmod n \quad (11)$$

However, to obtain  $\tilde{a}_1$  from Eq. (11) is actually a quadratic root problem. Without knowing the factors  $p, q$  of  $n = pq$ , it is hard for the adversary  $\mathcal{A}$  to obtain  $\tilde{a}_1$  from Eq. (11). As a result, the new online/offline Rabin signature is secure against the existential forgery attack.

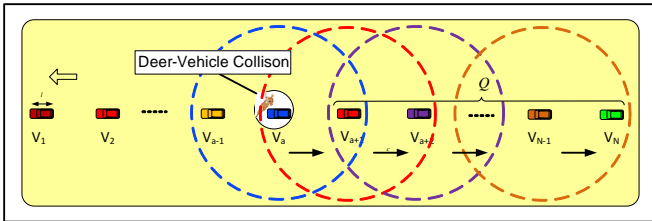


Fig. 3. Authenticated Emergence Message Propagation.

## V. MODELING AUTHENTICATED EMERGENCE MESSAGE PROPAGATION IN HIGHWAY TRAFFIC

In this section, we model the authenticated emergence message propagation in highway traffic to quantitatively analyze the effect of online/offline signature on the propagation delay.

We assume that a vehicle-cluster  $\mathcal{VC}$  is moving at the average velocity  $v$  in the proposed model, in which there are totally  $N$  vehicles  $\{V_1, V_2, \dots, V_N\}$ , as shown in Fig. 3. Suppose that a sudden deer-vehicle collision takes place at the  $a$ -th vehicle  $V_a$ , where  $1 \leq a \leq N$ . The vehicle  $V_a$  will immediately generate an authenticated emergence message  $m$  and broadcast it to the whole vehicle-cluster  $\mathcal{VC}$ . As the case stands in Fig. 3, when the deer-vehicle collision happens at  $a$ -th vehicle, those vehicles  $V_1, V_2, \dots, V_{a-1}$  ahead of  $V_a$  will not be affected. Therefore, the model actually should capture how fast an authenticated emergence message is propagated to the rest  $Q = N - a$  vehicles  $V_{a+1}, V_{a+2}, \dots, V_{a+Q}$  in the cluster.

TABLE I  
SOME NOTATIONS USED IN THE ANALYSIS

Notation	Definition
$v$	average velocity of each vehicle within $\mathcal{VC}$
$d_i$	hard-brake deceleration rate of vehicle $V_i$ within $\mathcal{VC}$
$T_{RD_i}$	brake response time of vehicle $V_i$ within $\mathcal{VC}$
$T_{PD_i}$	accident perception time of vehicle $V_i$ within $\mathcal{VC}$
$L_i$	distance between two neighboring vehicles $V_i$ and $V_{i+1}$
$l_i$	length of vehicle $V_i$ within $\mathcal{VC}$ , $l_i \ll L_i$
$R$	transmission range of vehicle within $\mathcal{VC}$ , $L_i \leq R$
$T_{TD}$	transmission delay caused by each message relay
$T_{SD}$	authentication delay caused by message signing
$T_{VD}$	authentication delay caused by message verification
$p$	success transmission probability

Before modeling the propagation, we first summarize some notations used in the analysis in Table I. When the deer-vehicle collision occurs, the vehicle  $V_a$  immediately generates and broadcasts an authenticated emergence message  $m$  in  $\mathcal{VC}$ . If the broadcast failure occurs,  $V_a$  rebroadcasts  $m$  until its success. Since the transmission range  $R_i$  satisfies  $L_i \leq R$  and  $l_i \ll L_i$ , the first broadcast can cover the neighboring vehicles within the transmission range, i.e., vehicle  $V_{a+1}$  will receive the emergence message. After checking the validity of the emergence message, vehicles  $V_{a+1}$  will follow the Algorithm 1 to make the 2-th hop broadcast. Later, with the same propagation policy in the Algorithm 1, the authenticated emergence message will be broadcasted continuously until all  $Q$  vehicles in  $\mathcal{VC}$  have received the current authenticated emergence message.

**Neighboring stopping distance (NSD).** The metric NSD captures whether a vehicle collision will occur between two neighboring vehicles  $V_i$  and  $V_{i+1}$ , and is defined as

$$\text{NSD} = \text{Pos}_i - \text{Pos}_{i+1} \quad (12)$$

where  $\text{Pos}_i, \text{Pos}_{i+1}$  are the stopping positions of the front vehicle  $V_i$  and the next vehicle  $V_{i+1}$ , respectively. If  $\text{NSD} > 0$ ,

---

**Algorithm 1** Emergence Message Propagation

---

```
1: procedure EMERGENCEMESSAGEPROPAGATION
2:   Upon receiving the authenticated emergence message  $m$ ,
   vehicle  $V_i$  checks its validity.
3:   if the authenticated emergence message  $m$  is valid then
4:     vehicle  $V_i$  begins to hard brake
5:     vehicle  $V_i$  concatenates its brake information  $m_i$  on  $m$ ,
   i.e.,  $m = m||m_i$ , and makes a new signature on  $m$ 
6:     vehicle  $V_i$  broadcasts the new authenticated emergence
   message  $m$ 
7:     while broadcast failure do
8:       vehicle  $V_i$  rebroadcasts  $m$ 
9:     end while
10:  else
11:     $V_i$  ignores the bogus message  $m$ 
12:  end if
13: end procedure
```

---

the vehicle collision can be avoided. Otherwise, the vehicle collision will occur.

Suppose that both  $V_i$  and  $V_{i+1}$  are within the transmission range of  $V_{i-1}$  and the relative distance between them is  $L_i$ . After receiving the authenticated emergence message from  $V_{i-1}$ , vehicles  $V_i$ ,  $V_{i+1}$  begin hard-braking almost simultaneously. Then, the stopping distance  $SD_i$  of  $V_i$  is the sum of the brake response distance  $RD_i$  and the braking distance  $BD_i$ , i.e.,

$$SD_i = RD_i + BD_i = v \cdot T_{RD_i} + \frac{v^2}{2d_i} \quad (13)$$

Correspondingly,  $SD_{i+1}$  of  $V_{i+1}$  is

$$SD_{i+1} = RD_{i+1} + BD_{i+1} = v \cdot T_{RD_{i+1}} + \frac{v^2}{2d_{i+1}} \quad (14)$$

Then, the neighboring stopping distance NSD between  $V_i$  and  $V_{i+1}$  can be expressed as

$$\begin{aligned} \text{NSD} &= \text{Pos}_i - \text{Pos}_{i+1} = SD_i + L_i - SD_{i+1} \\ &= L_i + v \cdot (T_{RD_i} - T_{RD_{i+1}}) + \frac{v^2}{2d_i} - \frac{v^2}{2d_{i+1}} \end{aligned} \quad (15)$$

When  $V_{i+1}$  is beyond the transmission range of  $V_{i-1}$ , based on the Algorithm 1, the accident perception time  $T_{PD_{i+1}}$  of  $V_{i+1}$  is the sum of  $V_i$ 's signing time  $T_{SD}$ ,  $V_{i+1}$ 's verification time  $T_{VD}$  and the transmission delay  $u \cdot T_{TD}$  after  $u$  times of broadcasts, where  $u \geq 1$ . Then, the stopping distance  $SD_{i+1}$  of  $V_{i+1}$  is the sum of the accident perception distance  $PD_{i+1}$ , the brake response distance  $RD_{i+1}$  and the braking distance  $BD_{i+1}$ , i.e.,

$$\begin{aligned} SD_{i+1} &= PD_{i+1} + RD_{i+1} + BD_{i+1} \\ &= v \cdot T_{PD_{i+1}} + v \cdot T_{RD_{i+1}} + \frac{v^2}{2d_{i+1}} \\ &= v \cdot (T_{SD} + T_{VD} + u \cdot T_{TD} + T_{RD_{i+1}}) + \frac{v^2}{2d_{i+1}} \end{aligned} \quad (16)$$

Therefore, NSD will be expressed as

$$\begin{aligned} \text{NSD} &= L_i + v \cdot (T_{RD_i} - T_{RD_{i+1}} - T_{SD} - T_{VD} \\ &\quad - u \cdot T_{TD}) + \frac{v^2}{2d_i} - \frac{v^2}{2d_{i+1}} \end{aligned} \quad (17)$$

## VI. PERFORMANCE EVALUATION

In this section, we validate the proposed propagation model and evaluate the performance of the proposed online/offline Rabin signature. Especially, we will discuss how the proposed online/offline Rabin signature scheme affects the chain reaction collision in highway traffic using a simulator built in Java. The metric we consider in the simulation is the *collision rate (CR)*, which is defined as

$$CR = \frac{\text{the number of chain-reaction collisions}}{\text{the total number of deer-vehicle collisions}} \quad (18)$$

We assume the OBUs equipped at the vehicles have 1.4 GHz processors for signature operations in software. Then, Table II illustrates our estimation of running time for 1024-bit RSA signature and the proposed online/offline Rabin signature, and the parameters in the table will be used for delay evaluation.

TABLE II  
ESTIMATED RUNNING TIME

Signature	RSA ( $e = 65537$ )	Online/offline Rabin
(online) signing ( $T_{SD}$ )	52.235 ms	0.011 ms
verification ( $T_{VD}$ )	0.811 ms	0.020 ms

### A. Simulation Settings

In highway traffic, it is important to keep a safe distance between two vehicles. Since if two vehicles are too close, the vehicle collision will occur with a high probability. Generally, the average vehicle distance in highway is estimated as 80 m. However, some cautious drivers keep a longer distance, while others prefer to a slightly shorter distance. In our simulation setting, we assume that the inter-vehicle distance follows the normal distribution  $\mathbb{N}(\mu, \sigma^2)$ , where  $\mu = 80$  m,  $\sigma = 20$  m. In addition, the transmission delay  $T_{TD}$  is configured 20 ms considering the latency of network and maximum number of repetitions in the network [8]. By statistics, we note that, when a sudden deer-vehicle collision occurs, if the vehicle chain-reaction collision doesn't take place in the direct-following  $Q$  vehicles, where  $Q \leq 10$ , it almost doesn't occur to the rest vehicles with a high probability, since the size of vehicle-cluster in highway traffic is usually less than 10. Therefore, in our delay evaluation, we only discuss the cases that  $Q \leq 10$ . The detailed parameter settings are listed in Table III. Then, we run the experiments with different parameters. For each experiment, we first generate 10,000 random deer-vehicle collision scenarios, and then count the number of chain-reaction collisions. We run each experiment 10 times, and the average collision rates are reported.

### B. Simulation Results

In Fig. 4, we compare the *collision rates CR* among the message propagation *without authentication*, *with the proposed online/offline Rabin signature* and *with RSA signature* when the parameter  $Q$  increases from 1 to 10. From the figure, we can see that  $CR$  in the proposed online/offline Rabin signature is less than that of RSA signature and almost consistent with

TABLE III  
PARAMETER SETTINGS

Parameter	Setting
$v$	[90 km/h, 100 km/h, 110 km/h, 120 km/h]
$d_i$	$8 \pm 2$ m/s <sup>2</sup>
$p$	90%
$L_i$	$\mathcal{N}(\mu, \sigma^2)$ , where $\mu = 60$ m, $\sigma = 20$ m
$R$	[100 m, 200 m]
$T_{RD_i}$	$1 \pm 0.5$ s
$T_{TD}$	20 ms
$T_{SD}$	[0 ms (no signing), 52.235 ms (RSA), 0.011 ms (Rabin)]
$T_{VD}$	[0 ms (no verification), 0.811 ms (RSA), 0.020 ms (Rabin)]

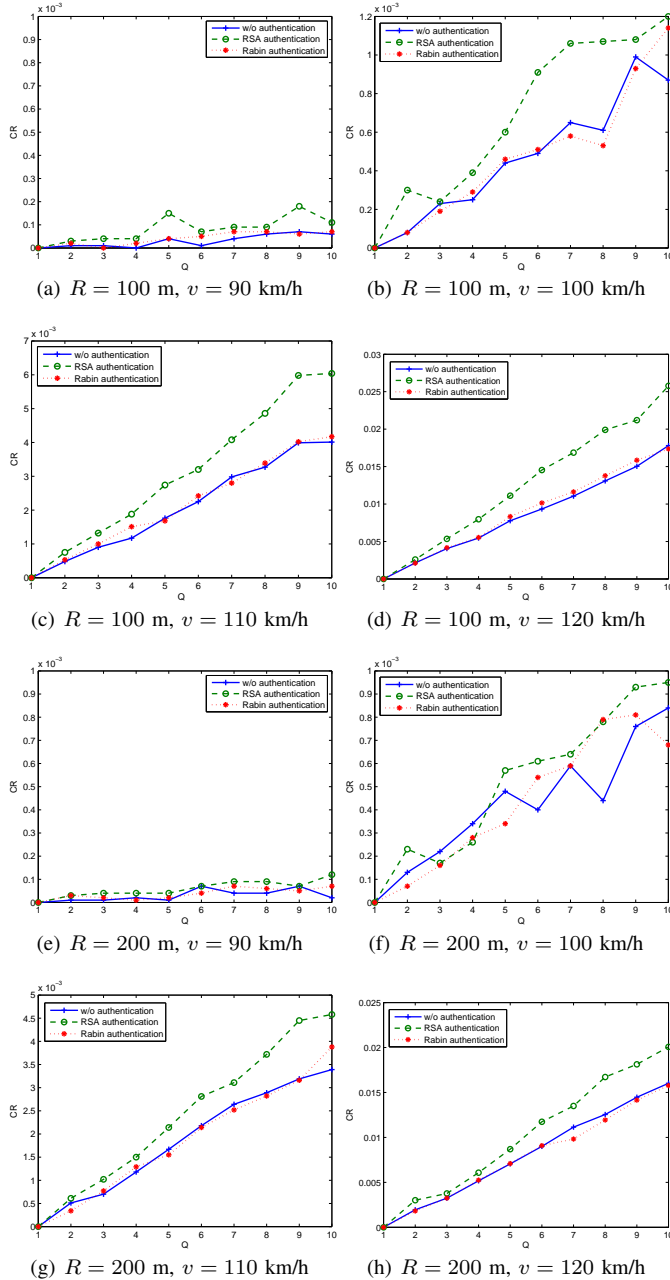


Fig. 4. The collision rate CR versus different parameter  $Q$ .

the CR without authentication in all settings. Although the CR gap between Rabin and RSA authentications is not big, it can effectively reduce some personal injuries and property damages. In addition, Fig. 4 also shows that the higher the velocity, the larger the CR. However, with the increase of the transmission range  $R$ , the CR will decrease.

## VII. CONCLUSIONS

Fast emergence message propagation is crucial to the success of mitigating the chain-reaction collision caused by a sudden deer-vehicle collision. In this paper, we have proposed a new online/offline Rabin signature scheme and modeled the emergence message propagation in highway traffic. We have demonstrated the effectiveness of the proposed scheme, i.e., the collision rate CR in the proposed scheme is less than that in RSA authentication, and almost consistent with the that without authentication. Our future work will focus on investigating more complex emergence message propagation model, which will involve vehicles in the neighboring lanes, since they could also be affected by a sudden deer-vehicle collision.

## REFERENCES

- [1] D. Muarray and D. Helden, "A proposal to develop a deer-vehicle collision reduction initiative", <http://www.public.iastate.edu/codi/Deer/proposal.pdf>
- [2] Strieter-Lite - Deer and Wildlife Warning Highway Reflectors, <http://www.strieter-lite.com/>
- [3] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho and X. Shen, "Security in vehicular ad hoc networks", *IEEE Communications Magazine*, Vol. 46, No. 4, pp. 88-95, 2008.
- [4] R. Lu, X. Lin, H. Zhu, P.-H. Ho and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications", in *INFOCOM 2008*, Phoenix, Arizona, USA, April 15-17, 2008.
- [5] X. Lin, X. Sun, P.-H. Ho and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communication", *IEEE Transactions on Vehicular Technology*, Vol. 56, No. 6, pp. 3442-3456, 2007.
- [6] R. Lu, X. Lin, H. Zhu and X. Shen, "SPARK: a new vanet-based smart parking scheme for large parking lots", in *INFOCOM 2009*, Rio de Janeiro, Brazil, April 19-25, 2009.
- [7] G. Resta, P. Santi, and J. Simon, "Analysis of multi-hop emergency message propagation in vehicular ad hoc networks", in *ACM MobiHoc 2007*, pp. 140-149, Montreal, Quebec, Canada.
- [8] S. Oh, J. Kang, M. Gruteser, "Location-Based Flooding Techniques for Vehicular Emergency Messaging", in *Proc. of Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, pp. 1-9, July 2006.
- [9] C. Tsai and W. Du, "Enhancement of delivery of warning messages for mobile networks", *Journal of Networks*, Vol. 3, No. 7, pp. 16-25, July 2008.
- [10] W. Mao, *Modern Cryptography: Theory and Practice*, Prentice Hall PTR, 2003.
- [11] S. Even, O. Goldreich, and S. Micali, "On-line/off-line digital signatures", in *Advances in Cryptology: Crypto' 89*, pp. 263-277, 1990.
- [12] A. Shamir and Y. Tauman, "Improved online/offline signature schemes", in *Advances in Cryptology: Crypto' 01*, pp. 355-367, 2001.
- [13] M. O. Rabin, "Digitized signatures and public-key functions as intractable as factorization," *MIT Lab. Comput. Sci.*, Cambridge, MA, Tech. Rep. LCS/TR-212, 1979.
- [14] R. Lu and Z. Cao, "Efficient remote user authentication scheme using smart card", *Computer Networks*, Vol. 49, No. 4, pp. 535-540, 2005.
- [15] X. Dong, R. Lu, and Z. Cao, "Proofs of security for improved Rabin signature scheme", *Journal of Shanghai Jiaotong University (Science)*, Vol. E-11, No. 2, pp. 197-199, 2006.