Efficient and Secure Message Authentication in Cooperative Driving: A Game-Theoretic Approach

Lei Gao, Na Ruan*, Haojin Zhu

Shanghai Jiao Tong University, China

***Abstract*—Requirement of safety, roadway capacity and efficiency in vehicular network, which makes autonomous driving concept continue to be of interest. To achieve automated cooperative driving, vehicles form a platoon. For the authentication in vehicular platoons, efficiency and security are the two things of great significance. Cooperative authentication is a way to help recognize false identities and messages as well as saving resources. However, selfish behaviors of the vehicles may be caused by the concern of privacy leakage and unfair resources consuming. To deal with these weaknesses, we devised an enhanced cooperative authentication protocol based on mechanisms which discourages non-cooperating behavior. An infinitely repeated game for our designed protocol in is proposed to analyze the utility of all users to help analyse the threat of selfish behavior. We also proposed a method to optimize the system parameters in our designed protocol to achieve better efficiency and security.**

***Index Terms*—Vehicular Platoons, Cooperative authentication, Game theory, Selfishness.**

I. Introduction

Autonomous driverless cars have recently received much publicity with successful demonstrations by Google, whose self-driving car has completed over 700,000 autonomous-driving miles across cities in the United States [1]. The vehicular platooning, wherein a group of vehicles act as a single unit through cooperative driving mechanisms, is expected to be a promising solution for self-driving cars. Cooperative driving means vehicles need to have access to each others information. An appropriately managed platoon can potentially offer enhanced safety, improved highway vehicle density, increased fuel economy, and reduced emissions [2].

In vehicular platoons, the vehicles utilize a one-vehicle look-ahead communication scheme. Each vehicle listens to the beacon messages sent wirelessly using IEEE 802.11p from its immediately preceding vehicle. Speed, position, acceleration, and other information are embedded in these beacon messages [3]. PTP (Precision Time Protocol, IEEE1588) is used to synchronize the clocks in V2V nodes to achieve a common notion of time. With the help of time synchronization, vehicles in the platoon are able to have a common knowledge of the common messages they need to authenticate at the same period of time, which founds as the precondition of cooperative message authentication.

Though there are quite a few studies which have been paid to the researches on transportation impacts, mechanical and control concerns, few attention has been paid to the security issues of vehicular platooning. Researchers pointed out that a malicious attack can mislead the other nodes by broadcasting the forged messages, which may cause the preceding car to collide and result in loss of life and assets [4]. It is also pointed out that the attacker can theoretically be capable of gaining control over the individual position and velocity (states) of other vehicles in the platoon [5]. The existing work proposed to enhance the system reliability of vehicular platooning via model-based abnormal detection scheme [6] cannot provide a systematic solution for message authentication as well as misbehavior preventing.

Achieving message authentication in vehicular platoons has to face several challenges. Firstly, smart driving applications like adaptive cruise control add to the burden of message authentication. Secondly, traditional message and user authentication faces the threat of insider attack, which may induce bad consequence like Collision Induction Attack [6]. Lastly, some researchers proposed communication protocols using cooperative authentication, which were carried out by a set of neighboring users timed to scheme which minimizes redundant authentication efforts of different users working on the same message [7–9]. Cooperative authentication did greatly cut the authentication cost, however, it may face the challenge of the existence of selfish nodes. In particular, the individual nodes may be reluctant to join the collaborative authentication to save the precious computational and communication resources [10].

To address the mentioned challenges, we propose a Cooperative Message Authentication and misbehavior Detection framework, coined as CMAD, to address various security vulnerabilities brought by falsified messages or selfish behavior. We use the game theoretical mode of n player infinitely repeated game to find out the factors that make the user behave selfishly and help improve the performance of our proposed protocol. We also perform extensive simulations to evaluate the efficiency and the effectiveness of the proposed framework.

The remainder of this work is organized as follows. In Section II, we briefly introduces the relevant background knowledge, including cooperative message authentication and infinitely repeated game. In section III, we proposed our designed protocol. In section IV, we presented the game theoretical approach. In section V and section VI, we show the analysis and evaluation of our work. We draw a conclusion in section VII.

*Corresponding author, Email: naruan@cs.sjtu.edu.cn.

This work is supported by National Natural Science Foundation of China (NSFC) under grant number 61532013, 61272444, U1401253, U1405251 and 61411146001.

978-1-4799-6664-6/16/$31.00 ©2016 IEEE

II. Preliminaries

In this section we briefly introduce the cooperative message authentication in vehicular platoons and the definitions of infinitely repeated game.

A. Cooperative Message Authentication in Vehicular Platoons

The general idea of cooperative authentication in vehicular platoons are presented as shown in Figure 1. Consider x vehicles within the communication range of a vehicular platoon. At each period of time, every vehicle have y common messages which are indexed and attached with signatures for them to authenticate. To reduce redundancy in authentication, vehicle randomly authenticates certain number of signatures and sends out an integrated signature s containing the indexes of original signatures $s_i, .., s_j$ it has authenticated. By authentication integrated signature s instead of original signature $s_i, ..., s_j$, vehicles actually authenticate fewer signatures in total thus they can alleviate the authentication cost and cut the authentication delay. By cooperative authentication, a message is usually authenticated for more than one time by different vehicles, which can enhance the probability to discover malicious message.

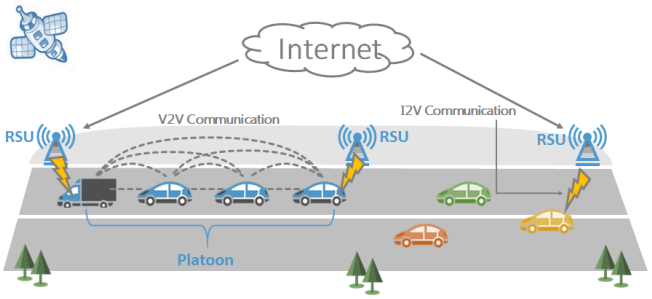

Fig. 1: Network Model

B. Infinitely Repeated Game

Definition 1. *Let a^t denote the action taken by player t. Let A^∞ represent the set of infinite sequences of action profiles. An infinitely repeated game is an extensive game with simultaneous form moves based on perfect information $< N, H, P, (\succeq_i^*) >$, where $H = \{\varnothing\} \cup (\bigcup_{t=1}^{\infty} A^t) \cup A^\infty$, P is a profile that maps every non-terminal history $h \in H$ to each player, $\succeq_i^*$ is a preference relation on A^∞ that satisfies the following notion of weak separability: if $a^t \in A^\infty, a \in A, a' \in A$ and $u_i(a) > u_i(a')$, then for all t, we have $(a^1, ..., a^{t-1}, a, a^{t+1}, ..) \succeq_i^* (a^1, ..., a^{t-1}, a', a^{t+1}, ..)$*

Definition 2. *A strategy profile σ is a Nash equilibrium if for every player i and every strategy σ_i',*

$$u_i(a(\sigma)) \geq u_i(a(\sigma_{-i}, \sigma_i'))$$

Definition 3. *A strategy profile σ is a subgame perfect equilibrium if it is a Nash equilibrium and for every history $h(t)$, every player i, and every alternative strategy σ_i'*

$$u_i(a(\sigma, h(t))) \geq u_i(a(\sigma_{-i}, \sigma_i', h(t)))$$

Definition 4. *Let $\Sigma \subseteq \mathbb{R}^N$ be a set of possible payoffs. For σ,$\sigma' \in \Sigma, if \exists \sigma_i' > \sigma_i$ and $\nexists \sigma_i' < \sigma_i$, then σ' Pareto dominates σ. Then $\sigma \in \Sigma$ is Pareto optimal if there exists no $\sigma' \in \Sigma$ for which σ_i' for all $i \in N$*

III. Efficient Cooperative Authentication Protocol

In this section, we introduce the details of our CMAD protocol.

A. Protocol Introduction

Based on the idea of cooperative authentication, we designed an efficient cooperative message authentication protocol. We use tokens to manage the process of verifying integrated signature. We use evidence to encapsulate the generated integrated signatures while token is used for decryption. We inherited an ID-based signcryption (IBSC) scheme[7] to control the capability of secure verification. We carried an optimization on the system parameters to further lessen the burden of generation integrated signatures.

B. Details

Our protocol consists of 7 parts.

1) Initialization and Setup: This step happens when the vehicular platoon is set up. The Lead Vehicle(LV) in the platoon chooses $\mathbb{G}$ and $\mathbb{G}_\mathbb{T}$ to be two finite cyclic groups of the same large order q. Suppose $\mathbb{G}$ and $\mathbb{G}_\mathbb{T}$ are equipped with a nondegenerated and efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_\mathbb{T}$ such that $\forall g, h \in \mathbb{G}, \forall a, b \in \mathbb{Z}_q, e(g^a, h^b) = e(g, h)^{ab}$ The LV chooses generator g of group $\mathbb{G}$. In addition, it also chooses random exponents $\mu \in \mathbb{Z}_q$ and two cryptographic hash functions $H : \{0,1\}^* \rightarrow \mathbb{G}$ and $H_1 : \mathbb{G}_2 \rightarrow \{0,1\}^N$. The LV sets $g_{pub} = g^\mu$. LV keeps a cooperation behavior record Rec. Rec is an n-bit number. $Rec_i = 1$ stands for vehicle i cooperated last time when it is requested to generate evidence while $Rec_i = 0$ stands for defect. Rec_i is initialized to 0. The system public parameters are $(\mathbb{G}, \mathbb{G}_\mathbb{T}, e, q, g, g_{pub}, H, H_1, N)$.

2) Join the Platoon: The LV assigns new coming vehicle i with pseudo identity pid_i with a secret key $psk_i = Q_i^\mu = H(pid_i)^\mu$.The LV set $Rec_i = 0$

3) Leave the Platoon: If LV is going to leave the platoon, LV sends the system parameter and Rec to the Potential Lead Vehicle(PLV).

4) Cooperation Request: At time slot t, the LV randomly pick k vehicles from n vehicles in platoon. Let $kv_t = \{pid_1|...|pid_{v_k}|s_t\}$, kv_t contains the picked vehicles' pseudo identity. LV send kv_t to the picked k vehicles. By sending kv_t, LV requires the k vehicles to generate integrated signatures (evidence). s_{t+1} is set by LV to specify the number of original signatures contained in one integrated signature.

5) Token Distribution: At time slot t, LV first checks if vehicle i in kv_t sends out evidence as required. If not, set $Rec_i = 0$. Else set $Rec_i = 1$. Then LV sends $tk_{t+1} = H(t+1)^\mu$ to vehicle i which $Rec_i = 1$. The token tk_{t+1} can be used to authenticate integrated signatures only at time slot $t+1$.

6) Evidence Generation: At time slot t, the vehicle randomly authenticates s_t original signatures. Let $MAC_{i,j}$ denote the one-bit authentication code of message id_j generated by vehicle i. Let $M_t = \{id_{i,1}|MAC_{i,1}, ..., id_{i,s_t}|MAC_{i,s_t}\}$. M_t denotes the necessary information that an integrated signature carries. Vehicle then chooses random number r_s,$r_e \in \mathbb{Z}_q$ Then it generates an integrated signature $s_{i,c} = (s_1, s_2)$ where $s_1 = g^{r_s}$,$s_2 = psk_i \cdot H(M_t)^{r_s}$ Then it broadcasts evidence $C_i(t) = \{(M_t||s_{i,c}) \oplus H_1(e(g_{pub}^{r_e}, H(t))), g^{r_e}\}$ to other vehicles in the platoon.

7) Cooperative Authentication: At time slot t, vehicle buffers the received evidence until all evidences are received or time slot t ends. When all evidence has arrived or time slot t ends, for each evidence $C_i(t)$, vehicle gets M_t and $s_{i,c}$ by $M_t||s_{i,c} = C \oplus H_1(e(g^{r_e}, tk_t))$. If $e(s_2, g) == e(H(pid_i), g_{pub}) \cdot e(H(M_t), s_1)$, get $id_{i,1}, ..., id_{i,s_t}$ and $MAC_{i,1}, ..., MAC_{i,s_t}$ from M_t . If evidence $C_i(t)$ does not arrive, the vehicle reports the misbehavior vehicle i to LV. For original message j, if all of its one bit authentication code $MAC_{i,j}$ is 1, then mark message j as successfully authenticated. If any $MAC_{i,j}$ is 0, then mark the message j as abnormal and report this abnormal to LV. Then authenticate the unmarked original messages. The cooperative authentication at time slot t is finished.

IV. Game Theoretical Analysis

In this section, we formulate an infinitely repeated game based on the cooperative authentication protocol. The key aspect of the game-theoretic analysis is to consider cost, privacy leakage and security as the utility of players to find out the condition under which players are willing to obey the protocol.

A. Infinitely Repeated Game Formulation

Suppose we have n vehicles in the platoon. During a certain time period, the platoon is stable without any vehicle joining in or leaving. At time slot t, the n vehicles are of two types. We name the vehicles which has token tk_t as type 1, the other as type 0. At each time slot, every vehicle will broadcast messages to vehicles in vehicular platoon. Also, infrastructures like RSU will also send messages to vehicles in platoon. We assume that the messages vehicles have in common is proportional to n. Let ny denote the messages vehicles have in common to authenticate. Each vehicle in platoon is a player in the game. Its strategy taken at time slot t can be presented as

$$a_i(t) = \{C, D\} \tag{1}$$

where C stands for generate evidence as required and D stands for not to generate evidence. At each time slot, vehicles in the platoon choose their strategy from their action space and play the stage game. Since vehicle platoon is dynamic, vehicles don't know how long they will last in the game. The stage game is infinitely played. We name the infinitely repeated game of each vehicle decide whether to take part in cooperative authentication as $G(T)$.

Let δ be the discounting rate which can be interpreted as the probability of a vehicle to stay in the game after one time slot. To build the utility system, first, we need to quantify the authentication cost.

Assume at time slot t, there are $X(t)$ vehicles choose the strategy C except player i. Let $x(t)$ denote the number of players who play strategy C at time slot t. Let C_v denote the cost of authenticating one signature. Let C_s be the cost of generating and transmitting one evidence. Let $s(t)$ be the original signatures contained in a single integrated signature at time slot t. Let P be the privacy value of a vehicle. Location privacy metric will involve topology feature of road condition. However, platoons drive on highways where the topology feature of road conditions is simple and consistent. Hence, without loss of generality, we can assume P to be a constant.

In addition, we have a type transition rule in this game.

$$Type_i(t+1) = \begin{cases} 1 & if\ pid_i \in kv_t\ and\ a_i(t) = C \\ 0 & if\ pid_i \in kv_t\ and\ a_i(t) = D \\ Type_i(t) & if\ pid_i \notin kv_t \end{cases} \tag{2}$$

Finally, we quantify the authentication cost in TABLE I. Besides authentication cost, the enhancement of security also plays an important part in the decision making of players. Suggest each vehicle has probability p_d to successfully detect a falsified message on its own. Let p_c denote the detection probability with cooperative authentication. Then $p_e = p_c - p_d$ denotes the enhancement of cooperative authentication. Let $ES(t)$ denote the security enhance of a player at time slot t. Let $D = \gamma C_v$ denotes the damage of a message manipulating attack. We have

TABLE I: The Authentication Cost

Cost	$a_i(t) = C$	$a_i(t) = D$
$Type_i(t) = 0$	$nyC_v + C_s + P$	nyC_v
$Type_i(t) = 1$	$[x(t) - 1 + s(t) + ny - r(t)]C_v + C_s + P$	$(x(t)+ny-r(t))C_v$

$$ES(t) = \begin{cases} p_e \cdot D & if\ Type_i(t) = 1 \\ 0 & if\ Type_i(t) = 0 \end{cases} \tag{3}$$

The utility function is formulated bases on the quantification of authentication cost and security enhancement in the protocol. Let $u_i(t)$ be the stage game payoff for player i at time slot t. Since C_v, C_s, P are all positive constant. We have

$$C_s = \alpha C_v, P = \beta C_v \tag{4}$$

Notice that the lower authentication cost it is, the greater utility it has. We formulate $u_i(t)$ by

$$u_i(t) = ny + \frac{ES(t) - Authentication\ Cost(t)}{C_v} \tag{5}$$

Thus we have the utility as TABLE II

TABLE II: The Stage Game Utility

$u_i(t)$	$a_i(t) = C$	$a_i(t) = D$
$Type_i(t) = 0$	$-\alpha - \beta$	0
$Type_i(t) = 1$	$r(t)+1-\alpha-\beta-s(t)-x(t)+\gamma p_e$	$r(t)-x(t)+\gamma p_e$

Let U_i be the discounted average of per time slot payoffs. Then

$$U_i = (1-\delta)\sum_{t=0}^{\infty} u_i(t)\delta^t \tag{6}$$

B. Analysis of The Game Model

Let S be the strategy suggested by our protocol.

$$S = \begin{cases} C & \text{if required} \\ D & \text{otherwise} \end{cases} \tag{7}$$

Let AS denote a strategy that player i always play strategy S. Let A denote the strategy profile.

$$A = \{AS, ..., AS\} \tag{8}$$

For convenience, let a denote the utility of type 0 player plays C, b denote the utility of type 1 player plays C, c denote the utility of type 1 player plays D. Let p be the probability to be picked to generate integrated signatures. Since $s(t)$ is chosen based on n, α, β, γ, and these parameters are constant in $G(T)$. We have $s = s(0) = ... = s(t)$. And in the same way we have $r = r(0) = ... = r(t)$. Player i's deviation from strategy S has two possible cases:

1) play D when required by LV.
2) play C when not required.

Since

$$c - b > 0 \Longleftrightarrow \alpha + \beta + s - 1 > 0 \rightarrow true$$

Hence, deviation from strategy S happens only in the case that player i refuse to play C when required by LV. Let DEV_N denotes the strategy that a vehicle deviates from S for N times continuously.

Lemma 1. *For player i, when $a_{-i} = \{AS, AS, ..., AS\}$, strategy DEV_{N+1} is less profitable than DEV_N*
Proof. Let time slot 0 be the time when player i deviates for the N th time. Let $u_i(t)$ denote the utility if player i deviates for the $N+1$ th time. Let $u_i'(t)$ denote the utility if player i does not deviate for the $N+1$ th time. By inductive inference,

$$u_i(t) = u_i'(t), t = 0$$
$$u_i(t+1) = u_i'(t), t \geq 1$$

Then we have

$$U_i' > U_i \Longleftrightarrow \delta < 1 \rightarrow true$$

Therefore, DEV_N is more profitable than DEV_{N+1} strategies. In this way, DEV_1 is the most profitable strategy among DEV_N strategies.

Lemma 2. *For player i, when $a_{-i} = \{AS, AS, ..., AS\}$, strategy AS is more profitable than DEV_1*
Proof. Assume the first deviation happens at time slot 0.
If player i sticks to strategy S,

$$u_i(t) = (1-p)c + pb$$
$$U_i = (1-\delta)(\sum_{t=0}^{\infty} u_i(t)\delta^t) = (1-p)c + pb \tag{9}$$

If player i plays DEV_1
when $t = 0$, $u_i'(t) = c$
when $t \geq 1$

$$\begin{aligned} u_i'(t) =& (1-p)^t \cdot 0 + (1-p)^{t-1} \cdot pa + \\ & (1-(1-p)^t - (1-p)^{t-1})(pb + (1-p)c) \\ \stackrel{def}{=}& u + v(1-p)^{t-1} \end{aligned} \tag{10}$$

where

$$u = pb + (1-p)c\ ,\ v = pa + (p-2)u \tag{11}$$

Thus

$$U_i' = (1-\delta)[c + \frac{u\delta}{1-\delta} + \frac{v\delta}{1-(1-p)\delta}]$$

Thus we have

$$U_i > U_i' \Longleftrightarrow \delta((c-u)(1-p) - v) > c - u$$

See that

$$c - u > 0 \Longleftrightarrow \alpha + \beta + s(t) > \frac{s(t)}{n}(1 - \frac{s(t)}{ny})^{x(t)} \rightarrow true$$

Therefore

$$U_i > U_i' \Longleftrightarrow \begin{cases} \delta > \dfrac{c-u}{(c-u)(1-p) - v} \stackrel{def}{=} td \\ p(c-u) + v < 0 \end{cases} \tag{12}$$

We suggest a function $J(k, s)$ that

$$J(k, s) = p(u - c) - v \tag{13}$$

Let tl denote time duration when a vehicle stays in platoon.

$$tl > \delta^0 + ... + \delta^\infty = \frac{1}{1-\delta} \geq \frac{1}{1-td} \stackrel{def}{=} T \tag{14}$$

When $J(k, s) > 0$ and $tl > T$, AS is more profitable than DEV_1

Theorem 1. *A is a subgame perfect Nash equilibrium of game $G(T)$.*
Proof. Let Z_n denote the strategy taken by player i in consecutive n time slots. By Lemma.1 and Lemma.2

$$\begin{aligned} & U_i(Z_n, DEV_N) < U_i(Z_n, DEV_1) < U_i(Z_n, AS) \\ \Longrightarrow\ & U_i(Z_{n-1}, Z_1, DEV_N) < U_i(Z_{n-1}, S, AS) \\ \Longrightarrow\ & U_i(Z_1, Z_1, ..., Z_1, DEV_N) < U_i(S, S, ..., S, AS) \end{aligned}$$

Since the strategy of player i can always be presented as $Z_1, Z_1, ..., Z_1, DEV_N$, the utility of strategy AS is greater than any other strategies. Hence every vehicle plays strategy AS is a Nash equilibrium.

Since we proved DEV_{N+1} is not more beneficial than DEV_N. DEV_1 is not more beneficial than AS. For any action history with deviation, one time deviation DEV_1 is not more beneficial than AS. According to One-Shot Deviation Principle[11], $ALL - S$ is subgame perfect.

Theorem 2. *A is Pareto optimal.*
Proof. According to the Nash folk theorem, there exists more

than one strategy which Nash equilibrium can be achieved in infinitely repeated games. For instance, strategies like Always Defect, Random Play, Grim Trigger etc. However, these strategies contain at least one deviation from cooperation. Since we proved in Theorem 1 that any deviation involved strategy is less beneficial than always cooperate. Therefore A is Pareto optimal.

V. Analysis on Cost and Security

In this section, we analyze on the performance of our CMAD protocol from aspects of efficiency and security. Previous work has proofed the correctness of the cryptographic aspect of the IBSC scheme which our protocol consists thus we focus the security analysis on game-theoretical terms.

A. Authentication Cost Formulation

Let k denote the number of vehicles taking part in generating integrated signatures. Let $Cost(k,s)$ be the cost of cooperative authentication of all n vehicles in one time slot.

$$\begin{aligned} Cost(k,s) =&[[k-1+s+ny-r+\alpha+\beta]k+ \\ &[k+ny-r](n-k)]]C_v \end{aligned} \tag{15}$$

where $1 \le k \le n, 1 \le s \le ny$, r is estimated by its Expection

$$r = E(r) = ny - ny(1-\frac{s}{ny})^k \tag{16}$$

Notice when using non-cooperative authentication, $Cost = n^2 y C_v$. In this way, the decrement rate of authentication cost per vehicle d can be presented as

$$d = 1 - \frac{Cost(k,s)}{n^2 y C_v} \tag{17}$$

B. Security Analysis

1) Message manipulating attack: An attacker in platoon may manipulate the message it receives and rebroadcast the manipulated malicious message. Cooperative authentication helps prevent this kind of message manipulating attack. Let ρ denote the malicious probability of vehicle. We have

$$p_c = \sum_{i=0}^{k} \binom{k}{i} \rho^i (1-\rho)^{k-i} [1-(1-\frac{s}{ny}\cdot p_d)^{k-i}] \tag{18}$$

2) Disobeying attack: A disobeying attack happens when a vehicle refuse to generate evidence required by the LV. By Lemma 2, we know $J(k,s) > 0$ and $tl > T$ is the two conditions that will make disobeying vehicles benefit less than obeying vehicles. By adjusting the system parameters we can make these two conditions true to make following the protocol best suits the benefit of vehicles.

3) Free-riding attack: Free-riding attack can be conducted passively or actively. Passive free-riding attack is conducted by vehicles making use of integrated signatures without making authentication efforts.

Since we require vehicles to use token tk to verify integrated signatures, where tk are provided for those vehicle whose $Rec = 1$. Thus vehicles without making authentication efforts are not able to make use of integrated signatures.

Active free-riding attack is conducted by vehicles pretends to contribute to cooperative authentication by incorporating nearby users' authentication efforts into its own integrated signature. Although this kind of attack has been solved by proposing an protocol that urges vehicle to generate authentication proof each time they generate evidence [7], it requires every vehicle to generate integrated signatures in order to be able to make use of their authentication efforts, which in turn heavy the burden of evidence generation.

To cope with active free-riding attack, we proposed a light weight attack detection scheme inspired by the idea of entrapment. At time slot t, LV sends out kv_t with a "ghost" vehicle id pid_i inside. Vehicle i is a virtual vehicle created by LV in vehicular platoons. Then at time slot $t+1$, LV sends s_t messages to vehicles on kv_t that can not be authenticated. Let fid_i denote the ids of those s_t messages. LV chooses random number r_s,$r_e \in \mathbb{Z}_q$, generates an integrated signature $s_{i,c} = (s_1, s_2)$, where $s_1 = g^{r_s}$,$s_2 = psk_i \cdot H(m_t)^{r_s}$. Then LV sends $C_i(t) = \{(m_t || s_{i,c}) \oplus H_1(e(g_{pub}^{r_e}, H(t))), g^{r_e}\}$ to those k vehicles. m_t contains those fid_i. Vehicles will tend to believe that this $C_i(t)$ is from vehicle i. Since vehicle j sends $C_j(t)$ to LV, if LV finds that fid_i is contained in $C_j(t)$, then vehicle j must be conducting free-riding attack.

This detection scheme succeeds at a probability. Consider one vehicle conducting free-riding attack in vehicular platoon. Let p_f denote the probability of successful detection.

Then

$$p_f = \begin{cases} 1 - \prod_{i=0}^{s} \frac{r-i}{r+s-i} & if\ r > s \\ 1 & otherwise \end{cases} \tag{19}$$

C. System Parameters Optimization

Here we propose a optimization of parameter k, s.

Algorithm 1 Optimization of k,s

```
procedure OPTIMIZATION(n, y, α, β, γ, ρ)
    for k from 1 to n do
        for s from 1 to ny do
            list(k, s) ← Cost(k, s)
        end for
    end for
    sort list in ascending order
    for each element in list do
        while T_p > p_d do
            if p_c > T_p and J(k, s) > 0 then
                return k, s
            end if
            T_p = T_p − 0.1
        end while
    end for
    return 0, 0
end procedure
```

The algorithm takes in system parameters $n, y, \alpha, \beta, \gamma, p_d$, user parameter T_p and outputs the optimal k, s pair. The marker states whether the output k, s pair can help resist selfish behavior of not following the protocol. The optimization is

done by filtering those k, s pair that has lower authentication probability than T_p. T_p is lowered if no k, s pair survives the filter. After the filtering, the k, s pair which generates the least amount of authentication cost is selected as output.

VI. Performance Evaluation

A. Evaluation Settings

Recent vehicular platoon project like SARTRE shows that in a vehicular platoon of 4 vehicles, a vehicle broadcasts 10 messages in each $25ms$. Thus we set $y = 10$ and time slot length $t = 25ms$. Generating and sending a evidence typically cost more than verifying a evidence. However, there is no method to quantify privacy, security, authentication cost on a common metric. Thus we set α, β,γ to make them basically as important as each other. p_d is set to 50%. This is because we assume vehicles have a mid-level ability of detecting the malicious message on its own.

In conclusion, we assume there are 2 to 15 vehicles in a vehicular platoon. Set $y = 10$, $\alpha = 10$, $\beta = 10$, $\gamma = 10$, $p_d = 0.5$. Time slot length is $25ms$. The other notations inherits from Section IV.

B. Evaluation Results

Before we carry out evaluation, we need to illustrate that $lt > T$ is easily satisfied. For each n from 2 to 15, we we calculated T with the setting above and we find that the largest $T = 534$. Since time slot length is $25ms$, $T \approx 14s$. In most practical cases, a vehicle stays in a platoon for more than 14 second. Then we give the stimulation results of algorithm 1 in Table III.

TABLE III: The Optimized Value of k,s

n	$T_p = 0.5$		$T_p = 0.7$		$T_p = 0.9$	
	k	s	k	s	k	s
2	1	20	1	20	1	20
3	1	30	1	30	1	30
4	2	30	2	33	2	33
5	2	40	3	37	3	47
6	2	50	3	45	3	56
7	2	60	3	52	4	69
8	2	70	3	59	4	78
9	2	80	3	67	4	88
10	2	90	3	74	4	98
11	2	100	3	81	4	107
12	2	98	3	89	4	117
13	2	120	3	96	4	127
14	3	103	3	103	4	137
15	2	140	3	111	4	146

By stimulating the free-riding attack detection probability p_f under the parameters given above, we find that : for any n from 2 to 15, we always have $p_f \to 1$. This shows that our free-riding attack detection scheme is successful.

Fig.2 shows the decrement rate of authentication cost when using the optimized algorithm. We can find that there is a trade-off between security and efficiency. If we set T_p higher, we will have lower authentication cost decrement. Notice that when $n = 2$, our protocol performs poorly in terms of efficiency. This indicates the applicability of our protocol. In all, when there are more than 2 vehicles, our protocol achieves both efficiency and security.

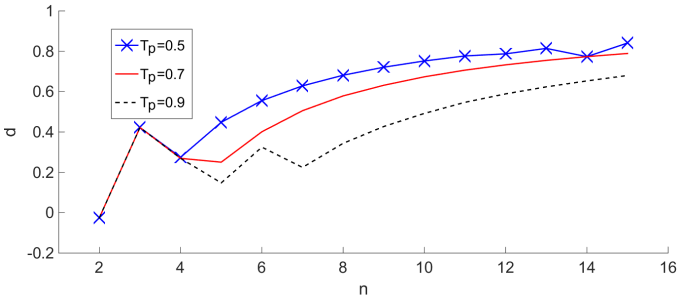

Fig. 2: Decrement Rate of Authentication Cost Per Vehicle

VII. Conclusion

In this paper, we proposed an effective cooperative message authentication protocol in vehicular platoons. By applying game theoretical analysis, we succeeded in proving that following the protocol mostly suits the interest of any vehicle itself. By performance analysis and evaluation, we proposed an optimization method on system parameters and successfully enhanced efficiency and security.

References

[1] J. Levinson, A. Jake, B. Jan, *Towards Fully Autonomous Driving: Systems and Algorithms*, in Proc. of IEEE Intelligent Vehicles Symposium (IV), 2011, pp. 163C68.

[2] L. Xu, L. Y. Wang, G. Yin and H. Zhang *Communication information structures and contents for enhanced safety of highway vehicle platoons*, IEEE Transactions on vehicular Technology, 2014, vol 63, no 9, pp 4206 -4220.

[3] C. Bergenhem, E.Hedin and D.Skarin, *Vehicle-to-vehicle communication for a platooning system*, Proc. Transp. Res. Arena, 2012

[4] M. Amoozadeh, A. Raghuramu, C. N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, K. Levitt, *Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving*, IEEE Communications Magazine, 2015, vol 53, no 6, pp 126-132.

[5] S. Dadras, R. M. Gerdes, R. Sharma, *Vehicular Platooning in an Adversarial Environment*, in Proc. of The 10th ACM Symposium on Information, Computer and Communications Security (ASIA CCS), 2015, pp 167-178.

[6] D.B. Bruce, W. Sean, S. Bruno and T. Patrick, *Is your commute driving you crazy?: a study of misbehavior in vehicular platoons*, in Proc. of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks(ACM WiSec), 2015, pp 22.

[7] X. Lin and X. Li. *Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks*. IEEE Transactions on Vehicular Technology, 2013, vol 62, no 7, pp 3339-3348.

[8] X Li, N Ruan, F Wu, J Li, M Li, *Efficient and enhanced broadcast authentication protocols based on multilevel TESLA*, 2014 IEEE International Performance Computing and Communications Conference (IPCCC), 2014, pp 1-8.

[9] R. Lu, X. Lin, H. Zhu, X. Liang and X. Shen, *BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks*, IEEE Transactions on Parallel and Distributed Systems, 2012, vol 23, no 1, pp 32-43.

[10] Y. Guo, L. Yin, L. Liu and B. Fang, *Utility-based Cooperative Decision in Cooperative Authentication*. in Proc. of The 33rd Annual IEEE International Conference on Computer Communications (INFOCOM14), 2014, pp 1006-1014.

[11] Tirole, D. Fudenberg ; Jean (1991). *Game theory* (6. printing. ed.). Cambridge, Mass. [u.a.]: MIT Press. ISBN 978-0-262-06141-4.