Securing Cooperative Adaptive Cruise Control in Vehicular Platoons via Cooperative Message Authentication

Na RUAN†, Nonmember, Chunhua SU††, Member, and Chi XIE†, Nonmember

SUMMARY The requirement of safety, roadway capacity and efficiency in the vehicular network, which makes vehicular platoons concept continue to be of interest. For the authentication in vehicular platoons, efficiency and cooperation are the two most important things. Cooperative authentication is a way to recognize false identities and messages as well as saving resources. However, taking part in cooperative authentication makes the vehicle more vulnerable to privacy leakage which is commonly done by location tracking. Moreover, vehicles consume their resources when cooperating with others during the process of cooperation authentication. These two significant factors cause selfish behaviors of the vehicles not to participate in cooperate cooperation actively. In this paper, an infinitely repeated game for cooperative authentication in vehicular platoons is proposed to help analyze the utility of all nodes and point out the weakness of the current collaborative authentication protocol. To deal with this weakness, we also devised an enhanced cooperative authentication protocol based on mechanisms which makes it easier for vehicles to stay in the cooperate strategy rather than tend to selfish behavior. Meanwhile, our protocol can defense insider attacks.

key words: vehicular platoons, cooperative authentication, game theory, selfishness, attack

1. Introduction

The vehicular platooning, wherein a group of vehicles act as a single unit through coordination of movements, is expected to be a promising solution for self-driving cars. By equipped with lower levels of function-specific automation such as cooperative adaptive cruise control (CACC) which makes use of a vehicle to vehicle communication, vehicles are grouped into platoons and drives autonomously or semi-autonomously. An appropriately managed platoon can potentially offer enhanced safety, improved highway vehicle density, increased fuel economy, and reduced emissions [1]. Vehicular platooning is increasingly attracting the interest of academia and the industry.

Though there are quite a few studies that 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. There has been a limited set of work that has explored the impact of attacks on platoon controllers. It is 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 [2]. Also, the attacker can theoretically be capable of gaining control over the individual position and velocity (states) of other vehicles in the platoon [3]. The existing work proposes to enhance the system reliability of vehicular platooning via model-based abnormal detection scheme [4], which cannot provide a systematic solution for message authentication as well as misbehavior preventing.

Securing cooperative adaptive cruise control in vehicular platoon through reliable message authentication has to face the following challenges. Firstly, Smart driving applications add to the burden of message authentication. Message authentication has been a fundamental security problem in Vehicular Ad hoc Networks (VANETs). Traditional Public Key Infrastructure (PKI)-based schemes may fail to satisfy the stringent time requirements of vehicular communication applications which may lead to the consequence of message loss and, in turn, pose a severe threat to the public safety. Secondly, with traditional user authentication, it can prevent the external attackers from injecting the modified messages while fail to thwart the insider attack, which may publish the legitimate but malicious letters inducing other vehicular nodes to make a wrong driving decision [4].

Lastly, some existing researches propose the concept of cooperative authentication, which is carried out by a set of neighboring vehicle users timed to scheme minimizes redundant authentication efforts of different vehicles working on the same message. However, cooperative authentication 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 precious computational and communication resources.

To address the above challenges, we propose a Cooperative Message Authentication and misbehavior Detection framework, coined as CMAD, to discuss various security vulnerabilities brought by the external attack, insider attack, and selfish nodes. The contribution of this work can be summarized as follows:

- To thwart the external attack, we propose a novel cooperative authentication scheme which can achieve highly efficient message authentication.
- To thwart the insider attack, we propose a novel neighborhood-based misbehavior detection scheme which leverages the nodes collaboration to achieve fast speed and position verification.
- To combat the selfish behavior attack, we introduce
a game theoretical based optimal strategy, which can help to resist selfish behavior.

We also perform extensive simulations to evaluate the efficiency and effectiveness of the proposed framework. The evaluations show that our protocol also has a high-efficiency enhancement.

2. Preliminaries

In this section, we introduce the basics of cooperative message authentication and infinitely repeated game.

2.1 Cooperative Message Authentication

Consider $x$ vehicles within the communication range of a vehicular platoon. At each period, every vehicle has $y$ common messages which are indexed and attached with signatures for them to authenticate. To reduce redundancy in authentication, vehicle randomly authenticates a certain number of signatures and sends out an integrated signature $s$ containing the indexes of original signatures $s_1, \ldots, s_j$ it has authenticated. By authentication integrated signature $s$ instead of original signature $s_1, \ldots, s_j$, vehicles authenticated fewer signatures in total thus attains less cost in authentication and cuts the authentication delay. By cooperative authentication, a message is usually authenticated for more than one time by different vehicles, which can enhance the probability of message authentication.

2.2 Infinitely Repeated Game

**Definition 1:** Let $a^t$ denote the action taken by player $t$. Let $A^\infty$ 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 $<_N H, P, (\succeq^*_t) >$, where

$$H = \{\emptyset\} \cup \left(\bigcup_{t=1}^{\infty} A^t\right) \cup A^\infty,$$

(1)

Here $N$ denotes the number of players. $P$ is a profile that maps every non-terminal history $h \in H$ to each player, $\succeq^*_t$ is a preference relation on $A^\infty$ that satisfies the following notion of weak separability: if $a' \in A^\infty, a \in A, a' \in A$ and $u_t(a) > u_t(a')$, then for all $t$, we have $(a^1, \ldots, a^{t-1}, a, a^{t+1}, \ldots) \succeq^*_t (a^1, \ldots, a^{t-1}, a', a^{t+1}, \ldots)$

**Definition 2:** A strategy profile $\sigma$ is a Nash equilibrium if for every player $i$ and every strategy $\sigma^*_i$,

$$u_i(\sigma) \geq u_i(\sigma_{-i}, \sigma^*_i)$$

(2)

Here the strategy profile $\sigma$ is the set of all player’s action, while $\sigma_i$ is the action of player $i$. $\sigma_{-i}$ is the strategy profile except player $i$. $u_i$ takes strategy profile as inputs and outputs the utility of player $i$.

At the Nash equilibrium, none of the players can prove its payoff by a unilateral deviation. The Nash equilibrium strategy is the best for a player if the others also use their Nash equilibrium strategies.

**Definition 3:** A strategy profile $\sigma$ is a subgame perfect equilibrium if it is a Nash equilibrium and for every history $h(t)$, every player $i$, and every alternative strategy $\sigma^*_i$

$$u_i(\sigma, h(t)) \geq u_i(\sigma_{-i}, \sigma^*_i, h(t))$$

(3)

For an extensive-form repeated game, strategies are played repeatedly to guarantee the Nash equilibrium at any subgame of the initial state game. The outcome is the subgame perfect equilibrium.

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

Typically, there is more than one equilibrium in the game. Therefore, it is important to define and evaluate a preference among equilibrium outcomes. A common approach is to measure optimality, which is called Pareto optimality. The Pareto optimality is the payoff profile that no strategy can make at least one player better off without making any other player worse.

3. Network Model and Attack Model

A vehicle platoon is a group of vehicles that travel within constant and close spacing to one another at a highway. A leading vehicle (LV) is followed by a number of following vehicles (FV) that closely match their speed and maneuvers to the leading vehicle. A platoon can start, stop, accelerate and decelerate as a unit and the ability to split, to allow the entry of vehicles and then rejoin as one platoon. We consider a vehicular platooning that is moving on a straight single-lane highway which is shown in Fig. 1. Each vehicle listens to the beacon messages sent wirelessly and then utilizes the speed, position, acceleration, and other information embedded in these beacon messages to achieve distributed longitudinal control [2].

In our protocol design, a time stamp is appended to the message authentication code to prevent the replay attack. Precision Time Protocol, IEEE1588 (PTP) is used to clocks in Vehicle to Vehicle (V2V) achieve a common notion of time. The communication protocol of V2V communication in vehicular platoon uses messages IDs for addressing rather than source-destination pairs as in the Ethernet.

![Fig. 1 Network model](image-url)
protocol. The source of a message is identified with an offset attached to it, thus makes it possible to discriminate the source of a V2V message. Time synchronization and message IDs make cooperative message authentication possible.

In this study, we consider the following attack models:

- **External attacks** For the external attacker, it can launch the Message Forgery Attack by impersonating a legitimate node to generate and broadcast fake beacon messages to mislead the other vehicles. The impact of such attacks can introduce temporary instability to the system. In some severe cases, it may lead to rear-end collision.

- **Insider attacks** For an insider attacker, the adversary can be a compromised vehicle with a valid certificate, which makes it difficult to detect and prevent.

- **Selfish behavior attacks** In the vehicular platooning, a selfish node may not follow the security protocol to avoid the extra security cost while still enjoy the security enhancement by receiving the security messages from other nodes. Selfish behavior will introduce unfairness to the system and discourage normal users from participating in security protocols.

### 4. Efficient Cooperative Authentication Protocol

In this section, we propose an efficient cooperative message authentication protocol in vehicular platoons.

#### 4.1 Notations

Here, we give notations of variables:

- \( n \): Number of vehicles in vehicular platoons.
- \( t_k \): The token for authentication at time slot \( t \)
- \( id_i \): The identity of the origin signature \( i \)
- \( pid_i \): The pseudo identity of vehicle \( i \)
- \( psk_i \): The secret key of the vehicle \( i \)
- \( s_t \): The number of original signatures covered in one integrated signature at time slot \( t \)
- \( s_{i,t} \): The integrated signatures generated by vehicle \( i \)
- \( C_i(t) \): Evidence generated by vehicle \( i \) at time slot \( t \)

#### 4.2 Protocol Description

Before introducing the protocol, we briefly look back our previous work [6, 7]. First, it is about efficient message authentication in a vehicular network. It is helpful against external attack but does not consider the insider attack, which gives us strong impetus to consider the situation of the cooperative.

##### 4.2.1 Efficient Message Authentication

To improve the authentication efficiency, we proposed a Paralleling Broadcast Authentication Protcol (PBAP) based on multi-level \( \mu \)-TESLA. The efficiency of PBAP mainly lies in the low cost of verifying MAC by symmetric keys and low cost of generating symmetric keys. A participating node can authenticate one message with one key at one time period. It reduced greatly of the authentication delay. It provides better serves for the propose of speeding up emergency data transmission in the vehicular network and better fits into the situation where vehicles are in RSU-sparse area.

##### 4.2.2 Efficient Cooperative Message Authentication

Cooperative message authentication is used to improve the efficiency in authentication, as, for most of the vehicles, the messages they need to authenticate are identical.

Based on the idea of cooperative authentication, we take the token to manage the process of verifying the integrated signature. We use evidence to encapsulate the generated integrated signatures while the token is used for decryption. We inherited ID-based encryption (IBSC) scheme to control the capability of verification, that is, secure verification of integrated signatures. We take a \( n - k \) scheme to further lessen the burden of generation integrated signatures.

#### 4.3 Details of Our Protocol

##### 4.3.1 Initialization and Setup

This step happens when the vehicular platoon is set up. The Lead Vehicle (LV) chooses \( G \) and \( G_2 \) to be two finite cyclic groups of the same large order \( q \). Suppose \( G \) and \( G_2 \) are equipped with a nondegenerated and efficiently computable bilinear map \( e : G \times G \rightarrow G_\tau \) such that \( \forall g, h \in G, \forall a, b \in \mathbb{Z}_q, e(g^a, h^b) = e(g, h)^{ab} \). The LV chooses generator \( g \) of group \( G \). In addition, it also chooses random exponent \( \mu \in \mathbb{Z}_q \) and two cryptographic hash functions \( H : \{0, 1\}^* \rightarrow G \) and \( H_1 : G_2 \rightarrow \{0, 1\}^N \). The LV sets \( g_{pub} = g^\mu \). LV keeps a cooperation behavior record \( Rec \). \( Rec \) is a \( n \)-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 \( (G, G_\tau, e, q, g, g_{pub}, H, H_1, N) \).
4.3.2 Join the Platoon

The LV assigns new coming vehicle $i$ with pseudo identity $pid_i$ with a secret key $psk_i = Q^e_i = H(pid_i)^y$. The LV set $Rec_i = 0$.

4.3.3 Leave the Platoon

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

4.3.4 Cooperation Request

We take an n-k scheme to lessen evidence generating a cost. At time slot $t$, The LV randomly pick $k$ vehicles from $n$ vehicles in a platoon. Name these vehicles as $PV_{t+1} = \{v_1, \ldots, v_k\}$. Let $kv_i = \{pid_i\} \ldots [pid_{i_0} | s_i]$. Here $||$ stands for concatenation. LV send $kv_i$ to each vehicle $v$ in $PV_{t+1}$. By sending $kv_i$, LV requires the $k$ vehicles included in $kv_i$ to generate integrated signatures (evidence). $s_{i+1}$ is sent along with the ids of required vehicles to specify the number of original signatures contained in one integrated signature. $s_{i+1}$ is chosen optimally to minimize the global authentication cost in vehicular platoons. The detailed explanation of $s_i$ is further discussed in Sect. 6. LV check if vehicle $i$ in $kv_{i-1}$ sends evidence. If not, set $Rec_i = 0$. Else set $Rec_i = 1$.

4.3.5 Token Distribution

At time slot $t$, LV sends $tk_{i+1} = H(t + 1)^y$ to vehicle $i$ which $Rec_i = 1$. The token can be used to authenticate integrated signatures only in time slot $t + 1$.

4.3.6 Evidence Generation

At time slot $t$, the vehicle randomly authenticate $s_i$ origin signatures. Let $MAC_{i,j}$ denote the one-bit authentication code of message $id_j$ generated by vehicle $i$. Let $M_i = [id_{i,1}|MAC_{i,1}, \ldots, id_{i,n}|MAC_{i,n}]$. $M_i$ denotes the necessary information that an integrated signature carries. Vehicle then choose random number $r_s, r_x \in \mathbb{Z}_q$ Then generates an integrated signature $s_{i,x} = (s_1, s_2)$ where $s_1 = g^{r_s}, s_2 = psk_i \cdot H(M_i)^{r_x}$. Then broadcast evidence $C_i(t) = \{M_i, s_{i,x}\} \oplus H_t(e(g^{r',p_{pub}}, H(t)))$ to other vehicles in the platoon.

4.3.7 Cooperative Authentication

At time slot $t$, vehicle buffer 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 $M_i$ and $s_{i,x}$ by $M_i|s_{i,x} = C \oplus H_t(e(g^{r'}, tk_i))$. If $e(s_2, g) = e(H(pid_i), g_{pub}) \cdot e(H(M_i), s_1)$, get $id_{i,1}, \ldots, id_{i,n}$ and $MAC_{i,1}, \ldots, MAC_{i,n}$ from $M_i$. If evidence $C_i(t)$ does not arrive, report 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. Report this abnormal to LV. Then authenticate the original unmarked messages. The cooperative authentication at time slot $t$ is finished.

5. Optimal Strategy against Selfishness

In this section, we will formulate an infinitely repeated game based on the cooperative authentication protocol.

5.1 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 have token $tk_i$ as type 1, the other as type 0, we have $Type(t) = \{0, 1\}$.

We assume that the messages vehicles have in common are proportional to $n$. Let $ny$ denote the messages vehicles have in common to authenticate. Each vehicle in the platoon is a player in the game. Its strategy taken at time slot $t$ can be presented as $a_i(t) = \{C, D\}$, where $C$ stands for generate evidence as required and $D$ stands for not to generate evidence. The strategy space can be presented as $A(t) = \{a_1(t) \times a_2(t) \times \ldots \times a_n(t)\}$.

At each time slot, vehicles in the platoon choose their strategy from their action space and play the stage game. The stage game is infinitely played. We name the infinitely repeated game of each vehicle to decide whether to take part in cooperative authentication as $G(T)$.

Let $\delta$ be the discounting rate which can be interpreted as the probability of a vehicle to stay in the game after a one-time slot. To build the utility system, we need to define the utility function at first. We first discuss the utility of player $i$.

We 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 $C$ denote the cost of authenticating one signature. Let $C_x$ 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. We can assume $P$ to be a constant, as platoons drive on highways where the topology feature of road conditions is consistent and straightforward.

In addition, we have a type transition rule in this game, and the authentication cost formulated in Table 1.

| $Type_i(t)$ | $a_i(t) = C$ | $a_i(t) = D$ |
|------------|---------------|---------------|
| 0          | $nyC_x + C_x + P$ | $nyC_x$ |
| 1          | $(s(t) - 1 + x(t) + ny - r(t))C_x + C_x + P$ | $(s(t) + ny - r(t))C_x$ |
Let $S_i$ be the strategy of player $i$ suggested by our protocol. We have

$$S_i = \begin{cases} C & \text{if $ pid_i \in kv_i$} \\ D & \text{if $ pid_i \notin kv_i$} \end{cases}$$

Let $AS$ denote a strategy that player $i$ always play strategy $S_i$. 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 $\beta, n, a, \alpha$, and these parameters are constant in $G(T)$. We have $s = s(0) = \ldots = s(t)$. And in the same way we have $r = r(0) = \ldots = r(t)$.

Player $i$'s deviation from strategy $S_i$ has two possible cases:

- play $D$ when required by $LV$.
- play $C$ when not required.

Since $c - b > 0 \iff a + \beta + s - 1 > 0 \rightarrow true$, deviation from strategy $S_i$ 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 $a_{-i} = \{AS, AS, \ldots, AS\}$, 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. If player $i$ deviates for the $N + 1$th time

$$u_i(0) = c$$
$$u_i(1) = 0$$
$$u_i(2) = pa + (1 - p) \cdot 0$$
$$u_i(3) = p^2b + p(1 - p)c + (1 - p)pa + (1 - p) \cdot 0$$
$$\ldots$$

If player $i$ does not deviate,

$$u'_i(0) = c$$
$$u'_i(1) = pa + (1 - p) \cdot 0$$
$$u'_i(2) = p^2b + p(1 - p)c + (1 - p)pa + (1 - p) \cdot 0$$
$$u'_i(3) = p^2b + p^2(1 - p)c + pb + (1 - p)c + (1 - p)p^2b + (1 - p)p(1 - p)c + (1 - p)^2pa + (1 - p)^3 \cdot 0$$
$$\ldots$$

By inductive inference, for $t \geq 1, u_i(t+1) = u'_i(t)$

$$U'_i = (1 - \delta) \sum_{t=0}^{\infty} u'_i(t)\delta^t = (1 - \delta)[c + \sum_{t=1}^{\infty} u'_i(t)\delta^t]$$

$$U_i = (1 - \delta) \sum_{t=0}^{\infty} u_i(t)\delta^t = (1 - \delta)[c + \sum_{t=1}^{\infty} u_i(t)\delta^t]$$

Then we have $U'_i > U_i \iff \delta < 1 \rightarrow true$. Therefore, $DEV_N$ is more profitable than $DEV_{N+1}$ strategies. By the way, $DEV_1$ is the most profitable strategy among $DEV_N$ strategies.

**Lemma 2:** For player $i$, when $a_{-i} = \{AS, AS, \ldots, AS\}$,

| $Type_s(t)$ | $a_i(t) = C$ | $a_i(t) = D$ |
|-------------|---------------|---------------|
| $Type_s(t) = 0$ | $-a - \beta$ | $0$ |
| $Type_s(t) = 1$ | $r(t) + 1 - a - \beta - s(t)$ | $r(t) - s(t) + \gamma p_r$ |

$$ES(t) = \begin{cases} p_e \cdot L & \text{if } Type_s(t) = 1 \\ 0 & \text{if } Type_s(t) = 0 \end{cases}$$

where $p_e$ denotes the enhance of authentication probability when using cooperative authentication. $L$ denotes the damage of an inside attack. Since $L$ is not correlated to any variables mentioned above, $L$ is a constant in this game model. For convenience, we can assume $L \gamma$ is the cost of the authentication cost of a single message. Then we have $L = \gamma C_e$.

The utility function is formulated based 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 $t$ which is also the $t$th stage game. Since $C_v, C_r, P$ are all positive constant. We have $C_s = \alpha C_v$ and $P = \beta C_r$. Notice that the lower authentication cost it is, the greater utility it has. We formulate $u_i(t) = ny + ES(t) - Authentication Cost(t)$. Thus we have the utility as Table 2.

| $u_i(t)$ | $a_i(t) = C$ | $a_i(t) = D$ |
|----------|---------------|---------------|
| $Type_s(t)$ | $-a - \beta$ | $0$ |
| $Type_s(t)$ | $r(t) + 1 - a - \beta - s(t)$ | $r(t) - s(t) + \gamma p_r$ |

5.2 Analysis of the Game Model

To explain the detail, there are $ny$ common messages for each vehicle to authenticate. Assume that the $x(t)$ integrated signature will cover $r(t)$ number of $ny$ signatures.

If $Type_s(t) = 0$, when player $i$ plays $D$, it has to authenticate $ny$ messages all by itself. When player $i$ plays $C$, it has not only authenticate $ny$ messages all by itself, but also generate and transmit one evidence. It will lose some privacy value when transmitting evidence.

If $Type_s(t) = 1$, when player $i$ plays $D$, it has to authenticate $x(t)$ integrated signature and those uncovered $ny - r(t)$ signatures. When player $i$ plays $C$, it has to authenticate $x(t) - 1$ integrated signature and those uncovered $ny - r(t)$ signatures plus generate and transmitting one evidence. It will lose some privacy value when transmitting evidence.

Besides authentication cost, the enhancement of security also plays an important part in the decision making of players. Let $ES(t)$ denote the security enhancement of a player at time slot $t$. We have

$$ES(t) = \begin{cases} p_e \cdot L & \text{if } Type_s(t) = 1 \\ 0 & \text{if } Type_s(t) = 0 \end{cases}$$

where $p_e$ denotes the enhance of authentication probability when using cooperative authentication. $L$ denotes the damage of an inside attack. Since $L$ is not correlated to any variables mentioned above, $L$ is a constant in this game model. For convenience, we can assume $L \gamma$ is the cost of the authentication cost of a single message. Then we have $L = \gamma C_e$.

The utility function is formulated based 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 $t$ which is also the $t$th stage game. Since $C_v, C_r, P$ are all positive constant. We have $C_s = \alpha C_v$ and $P = \beta C_r$. Notice that the lower authentication cost it is, the greater utility it has. We formulate $u_i(t) = ny + ES(t) - Authentication Cost(t)$. Thus we have the utility as Table 2.

| $u_i(t)$ | $a_i(t) = C$ | $a_i(t) = D$ |
|----------|---------------|---------------|
| $Type_s(t)$ | $-a - \beta$ | $0$ |
| $Type_s(t)$ | $r(t) + 1 - a - \beta - s(t)$ | $r(t) - s(t) + \gamma p_r$ |
strategy AS is more profitable than DEV\(_1\).

Proof. Assume the first deviation happens at time slot 0. If player \(i\) sticks to strategy \(S_i\), \(u_i(t) = (1 - p)c + pb\)

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

(9)

If player \(i\) plays \(DEV_1\), when \(t = 0\), \(u'_i(t) = c\), and when \(t \geq 1\)

\[
u'_i(t) = (1 - p)^t \cdot 0 + (1 - p)^{t-1} \cdot pa +
\]

\[\left(1 - (1 - p)^{t-1}\right)(pb + (1 - p)c)\]

\(\overset{\text{def}}{=} u + \nu(1 - p)^{t-1}\)

(10)

(11)

where \(u = pb + (1 - p)c\) and \(v = pa + (p - 2)u\). Thus

\[
U'_i = (1 - \delta)\left[ c + \sum_{t=1}^{\infty} u'_i(t) \delta^t \right]
\]

\[
= (1 - \delta) \left[ c + \frac{u\delta}{1 - \delta} + \frac{v\delta}{1 - (1 - p)\delta} \right]
\]

(12)

Thus we have \(U_i > U'_i \iff \delta((c - u)(1 - p) - v) > c - u\).

See that \(c - u > 0 \iff \alpha + \beta + s(t) > \frac{s(t)}{n} (1 - s(t))\) is true, \(U_i > U'_i \iff (1 - p - \frac{s(t)}{n})\delta > 1\). Since \(0 < \delta < 1\), we have \(1 - p - \frac{s(t)}{n}\delta > 1 \iff \rho(c - u) + v > 0\). Thus, we can suggest a function \(J(k, s)\) that \(J(k, s) = p(u - c) - v\). If \(J(k, s) > 0\) then

\[
\delta > \frac{c - u}{(c - u)(1 - p) - v} = \frac{c - b}{b - a + \left(\frac{2}{p} - 2\right)c} \overset{\text{def}}{=} \frac{t_l}{d_t}
\]

(13)

Let \(t_l\) denote the least time required for a vehicle to stay in platoon.

\[
t_l = \delta^0 + \ldots + \delta^\infty = \frac{1}{1 - \delta} \geq \frac{1}{1 - t_d} \overset{\text{def}}{=} T
\]

(14)

Since \(k, s\) are system variables that can be decided by LV; we can choose appropriate \(k, s\) to make \(J(k, s) > 0\). This is shown in Sect. 6. When \(J(k, s) > 0\), the stimulation shows that \(T\) is always a relatively small number which in practical scenes a vehicle always stays in the platoon for much more than \(T\) time slots. Therefore, \(AS\) is the more profitable than \(DEV_1\).

**Theorem 1:** \(A\) is a subgame perfect 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

\[
U_i(Z_n, DEV_N) < U_i(Z_n, DEV_1) < U_i(Z_n, AS)
\]

(15)

\[
U_i(Z_{n-1}, Z_1, DEV_N) < U_i(Z_{n-1}, S, AS)
\]

(16)

\[
U_i(Z_1, Z_1, \ldots, Z_1, DEV_N) < U_i(S, S, \ldots, S, AS)
\]

(17)

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

Since we proved \(DEV_{N+1}\) is not beneficial than \(DEV_N\), and \(DEV_1\) is not beneficial than \(AS\). For any action history with deviation, one-time deviation \(DEV_1\) is not beneficial than \(AS\). According to One-Shot Deviation Principle [9], \(ALL - S\) 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 the infinitely repeated game. 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.

### 6. Security Analysis

In this section, we give the analysis of the attacks given by the attack model.

#### 6.1 External Attacks

In Linkability attack, since an integrated signature contains the pseudonym secret key \(pski\), LV can make use of the key to identify the attacker. Linkability attack can be detected. While in Eavesdropping attack on privacy leakage, it can be prevented by protocol design. The LV can distribute new pseudo identities to the vehicles in the platoon, which the tracking difficult.

#### 6.2 Inside Message Manipulating Attack

An attacker in platoon may broadcast malicious message. Cooperative authentication helps prevent this kind of inside attack. Authentication probability denotes the probability with which a false message/identity are successfully recognized. Consider each vehicle has probability \(p_d\) to discover that a message is malicious or not on its own. Let \(p_e\) denote the authentication probability with cooperative authentication, and \(\rho\) denote the malicious probability of vehicle, we have

\[
p_e = \sum_{i=0}^{k} \binom{k}{i} \rho^i (1 - \rho)^{k-i} [1 - (1 - \frac{\delta}{n} - \rho \cdot p_d)^{k-i}] \]

(18)

#### 6.3 Selfish Behavior Attacks

For the selfish behavior attacks, we take the passive free-riding attack as an example. The passive free-riding attack is prevented by protocol design. We require vehicle use \(rk\) to verify integrated signatures, where \(rk\) are provided for those vehicle whose \(Rec\) = 1. Thus vehicles without making authentication efforts are not able to make use of integrated signatures.

For active free-riding attack, an protocol that urges vehicle to generate evidence each time they generate evidence [10], 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 evi-
dence generation.

To cope with the active free-riding attack, we proposed a lightweight attack detection scheme based on the idea of entrapment. At time slot $t$, LV sends $k v_i$ with a “ghost” vehicle id $p i d_i$ inside. Vehicle $i$ is a virtual vehicle created by LV in VANET platoons. Then at time slot $t + 1$, LV sends $s_i$ messages to vehicles on $k v_i$ that can not be authenticated. Let $f i d_i$ denote the ids of those $s_i$ messages. LV Choose random number $r_s, r_e \in Z_q$, generates an integrated signature $s_{i c} = (s_1, s_2)$, where $s_1 = g^{r_s}, s_2 = p s k_i \cdot H(m_i)^{r_e}$. Then LV sends $C_i(t) = \{m_i||s_{i c} \oplus H(\epsilon(q_{m_i}^w, H(t)))), g^{r_e}\}$ to those $k$ vehicles. $m_i$ contains those $f i d_i$. 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 find that $f i d_i$ 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 a free-riding attack in a vehicular platoon. Let $p_f$ denote the probability of successful detection, we can get that

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

7. Performance Evaluation

To give insight into the performance of the proposed secure cooperative authentication scheme, we have conducted a set of custom simulations using C++ and python. In the following, we detail our simulation settings and present the evaluation results.

7.1 Evaluation Settings

We set $y = 10$ and time slot length $t = 25ms$. Generating and sending evidence typically cost more than verifying evidence. However, there is no method to quantify privacy, security, authentication cost on a common metric. Thus we set $\alpha = 10, \beta = 10$ and $\gamma = 0.1$ to make them as important as each other. $p_d$ is set to $50\%$. This is because we assume vehicles have a mid-level ability to detect the malicious message on its own. In our evaluation, we set $n = 5, 10$ to represent the size of a common platoon and future larger platoon. Set $y = 10, \alpha = 10, \beta = 10, \gamma = 100, p_d = 0.5$. Time slot length is $25ms$.

7.2 Evaluation Results

7.2.1 Authentication Cost

Here we analysis on the authentication cost of cooperative authentication. Let $k$ denote number of FVs taking part in generating integrated signatures. Let $Cost(k, s) = \frac{[k - 1 + s + ny - r + \alpha + \beta]k + [k + ny - r(n - k)]C_i}{s}$, be the cost of cooperative authentication of all $n + 1$ vehicles in one time slot, in which $0 \leq k \leq n, 1 \leq s \leq ny$.

Figure 3 (a) and Fig. 3 (d) describe the relation between $k, s, cost$ when $n = 5, 10$. We can find that for any given $k$, with $s \rightarrow ny$, cooperative authentication cost first decrease than increase. For any given $s$, with $k \rightarrow N$, cooperative authentication cost increases. In most of the cases, cooperative authentication outperforms non-cooperative authentication. This shows a great enhancement of cooperative authentication in lessening authentication burden. When $s \rightarrow 0, k \rightarrow N$ or $s \rightarrow ny, k \rightarrow N$, non-cooperative authentication outperforms cooperative authentication. This indicates that cooperative authentication performs poorly when signatures which are cooperatively authenticated are too few or too many. To minimize authentication cost, we should pick smaller $k$ and larger $s$.

7.2.2 Authentication Probability

This part of the evaluation mainly discusses the authentication probability in our protocol. Here we fix $n = 10$ and consider two scenario when $\rho = 0.1, 0.7$, where $\rho = 0.1$ stands for a normal rate of malicious vehicle, $\rho = 0.7$ stands
for a highly illed vehicle platoon. Figure 3 (b) and Fig. 3 (e) describes the relation between \( p_c \) and \( k, s \). We can find that \( k, s \) are both positive correlation to \( p_c \), while \( s \) has a greater impact on \( p_c \). With \( s, k \) sufficiently large, we can achieve authentication probability almost 100\%. Since the original authentication probability \( p_d = 0.5 \) is relative low, cooperative authentication here has a great enhancement on security. Notice that when \( k = 1 \), the curve turn into line. This is because that the exponent of the exponential function becomes 0 thus turning the function into linear.

### 7.2.3 Nash Equilibrium

This part of evaluation lies in the condition it takes to reach the NE of cooperation behavior. For each \( n \) from 2 to 20, let \( f(k, s) = \frac{1}{n^2} \) and \( T = \max f(k, s) \), \( 0 \leq k \leq n, 0 \leq s \leq ny \). Here \( T \) stands for the maximum time of the least time required for a vehicle to stay in the platoon.

Figure 4 shows the relation between \( T \) and \( n \). We can find that the largest \( T = 2024 \), since time slot is 25ms, this means that a vehicle must stay in the platoon for at least 50 seconds. In a practical scenario, a vehicle stays in a platoon for more than 50 seconds in most cases. Therefore, for a common platoon of vehicles 2 to 20, it’s patience is always enough for it to play the strategy of cooperate. Hence, \( J(k, s) \) is the only possible constraint to NE.

Figure 3 (c) and Fig. 3 (f) shows the relation between \( J(k, s) \) and \( k, s \) when \( n = 5, 10 \). We can find that in most cases, \( J(k, s) > 0 \) is true. That means NE is possible in these cases. This ensures that our protocol can resist selfish behavior in most cases. Notice that NE is not reachable when \( k \rightarrow N, s \rightarrow Ny \). However, these cases are only of small proportion. Besides, the authentication cost will be very large when \( k \rightarrow N, s \rightarrow Ny \). There is no incentive of LV to choose such \( k, s \) that threats cooperation.

### 7.2.4 Free-Riding Attack Detection

This part of evaluation mainly shows the detection probability of our free-riding attack detection method. Figure 5 shows the successful detection probability of our proposed free-riding attack detection scheme. We can find that \( p_f \rightarrow 1 \) when \( s \rightarrow ny \). Further more, when \( s > 20 \), \( p_f \approx 1 \) regardless of \( k \). It is clear that \( s \) is the dominant factor of \( p_f \). Since it is common for \( s \) to be larger than 20, the detection is effective. This shows that our free-riding attack detection scheme is successful.

### 7.2.5 Balancing Efficient and Security

Finally, it comes to optimize the choice of appropriate \( k, s \). From evaluations above, we know that there is a trade-off between security and efficiency. Adding that not all \( k, s \) can ensure a NE of cooperation, the appropriate choice of \( k, s \) is a major concern in our protocol. Thus we need a method to decide the appropriate choice of \( k, s \) in vehicular platoons. Here \((k, s) = \arg\min_{(k,s)∈K} Cost(k, s) = \{(k, s) | p_c > T_p \land J(k, s) > 0\} \).

\( T_p \) is the threshold of authentication probability. For those \( k, s \) meeting the threshold and ensuring NE of cooperation, authentication cost is then minimized. Take \( T_p = 0.9 \), in this way we calculate the optimal \( k, s \) as shown in Table 3, where \( n \) denote the number of vehicles in a platoon, DC denote the Decrement Rate of Authentication Cost, AP denote the Authentication Probability. The authentication cost is greatly reduced. Notice, when \( n = 2 \) there is no possible NE, the table starts at \( n = 3 \). When \( n = 3, 4, 5, 6 \) there is no possible \( k, s \) that \( p_c > T_p \), so we choose the \( k, s \) that makes \( p_c \) most close to \( T_p \) which is not against our rule of security first.

### 8. Conclusion

In this paper, we proposed an effective cooperative message authentication protocol in vehicular platoons. We succeeded in proving that following our proposed protocol mostly suits the interest of any vehicle itself by applying game theoretical analysis. Besides, our protocol can efficiently reduce the authentication cost as well as resist some inside attacks by security analysis, which is significantly better than recent previous work.

### References

[1] L. Xu, L.Y. Wang, G. Yin, and H. Zhang, “Communication informa-
nation structures and contents for enhanced safety of highway vehicle platoons,” IEEE Trans. Veh. Technol., vol.63, no.9, pp.4206–4220, 2014.

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

[3] S. Dadras, R.M. Gerdes, and R. Sharma, “Vehicular Platooning in an Adversarial Environment,” Proc. 10th ACM Symposium on Information, Computer and Communications Security (ASIA CCS), pp.167–178, 2015.

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

[5] M.H. Manshiaei, Q. Zhu, T. Alpcan, T. Basar, and J.-P. Hubaux, “Game theory meets network security and privacy,” ACM Computing Surveys (CSUR), vol.45, no.3, p.25, 2013.

[6] M. Li, N. Ruan, H. Zhu, J. Li, and X. Li, “A Parallelized Broadcast Authentication Protocol for Sparse RSUs in Internet of Vehicles,” Proc. 10th International Conference on Mobile Ad-hoc and Sensor Networks (MSN), pp.58–65, 2014.

[7] X. Li, N. Ruan, F. Wu, J. Li, and M. Li, “Efficient and enhanced broadcast authentication protocols based on multilevel μTESLA,” Proc. IEEE International Performance Computing and Communications Conference (IPCCC), pp.1–8, 2014.

[8] R. Shokri, G. Theodorakopoulos, J.-Y.L. Boudec, and J.-P. Hubaux, “Quantifying location privacy,” IEEE Symposium on Security and Privacy (SP), pp.247–262, 2011.

[9] D. Fudenberg and J. Tirole, Game Theory, 6th ed., MIT Press, Cambridge, 1991.

[10] X. Lin and X. Li, “Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks,” IEEE Trans. Veh. Technol., vol.62, no.7, pp.3339–3348, 2013.

[11] Y. Hao, Y. Cheng, C. Zhou, and W. Song, “A distributed key management framework with cooperative message authentication in VANETS,” IEEE J. Sel. Areas Commun., vol.29, no.3, pp.616–629, 2011.

[12] Y. Hao, T. Han, and Y. Cheng, “A cooperative message authentication protocol in VANETS,” Proc. Global Communications Conference (GLOBECOM), pp.5562–5566, 2012.

[13] Y. Guo, L. Yin, L. Liu, and B. Fang, “Utility-based Cooperative Decision in Cooperative Authentication,” Proc. 33rd Annual IEEE International Conference on Computer Communications (INFCOM14), pp.1006–1014, 2014.

[14] T. Alpcan and S. Buchegger, “Security games for vehicular networks,” IEEE Trans. Mobile Comput., vol.10, no.2, pp.280–290, 2011.

[15] M. Prabhakar, J.N. Singh, and G. Mahadevan, “Defensive Mechanism for VANET security in game theoretic approach using heuristic based ant colony optimization,” Proc. International Conference on Computer Communication and Informatics (ICCCI), pp.1–7, 2013.

[16] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, “An efficient message authentication scheme for vehicular communications,” IEEE Trans. Veh. Technol., vol.57, no.6, pp.3357–3368, 2008.

[17] T. Chen, L. Wu, F. Wu, and S. Zhong, “Stimulating Cooperation in Vehicular Ad Hoc Networks: A Coalitional Game Theoretic Approach,” IEEE Trans. Veh. Technol., vol.60, no.2, pp.566–579, Feb. 2011.

[18] Y. Wang, F.R. Yu, M. Huang, A. Boukerche, and T. Chen, “Securing vehicular ad hoc networks with mean field game theory,” Proc. 3rd ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (DIIVANet 13), pp.55–60, 2013.

[19] B. LSlanchev, “Game theory: Repeated games,” Tech. Rep., Department of Political Science, University of California-San Diego, pp.1–19, March 2004.

[20] J. Freudiger, M.H. Manshiaei, J.-P. Hubaux, and D.C. Parkes, “Non-Cooperative Location Privacy,” IEEE Transactions on Dependable and Secure Computing, vol.10, no.2, pp.84–98, 2013.

[21] M. Prabhakar, J.N. Singh, and G. Mahadevan, “Nash Equilibrium and Marcov Chains to Enhance Game Theoretic Approach for VANET Security,” Proc. International Conference on Advances in Computing (ICAdC), pp.191–199, 2013.

[22] D.T. Hoang, X. Lu, D. Niyato, P. Wang, and Z. Han, “Applications of repeated games in wireless networks: A survey,” arXiv:1501.02886v1, Jan. 2015.

[23] T. Tithi, R. Gerdes, and C. Winstead, “Poster: Position verification in vehicular platoons using a Euclidean distance matrix,” Proc. Symp. Security and Privacy, May 2015.

Na Ruan is currently an Assistant Professor with Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. She received the B.S. degree in Information Engineering from China University of Mining and Technology and her Ph.D. degree from the Department of Information Science and Electrical Engineering, Kyushu University, Japan in 2007 and 2012, respectively. Her current research interests include AI/network security and privacy-preserving technologies.

Chunhua Su received the B.S. degree for Beijing Electronic and Science Institute in 2003 and received his M.S. and Ph.D. of computer science from Faculty of Engineering, Kyushu University in 2006 and 2009, respectively. He is currently working as an Associate Professor in Division of Computer Science, University of Aizu. He has worked as a research scientist in Cryptography & Security Department of the Institute for Infocomm Research, Singapore from 2011-2013. From 2013-2016, he has worked as an Assistant professor in School of Information Science, Japan Advanced Institute of Science and Technology. From 2016-2017, he worked as Assistant Professor in Graduate School of Engineering, Osaka University. His research interests include cryptanalysis, cryptographic protocols, privacy-preserving technologies in data mining and IoT security & privacy.

Chi Xie obtained his Ph.D. in Systems Engineering from Cornell University in 2008. He has been teaching at University of Texas at Austin, Shanghai Jiao Tong University and Tongji University over the past decade, and is currently a Professor in the School of Transportation Engineering at Tongji University. His research focuses on transportation network management and control, travel demand analysis and forecasting, electrified and shared transportation systems, and freight transportation and logistics systems, in which he is particularly interested in developing innovative methods to analyze and optimize large-scale urban and regional transportation systems on the strategic, tactical and operational levels.