Secure and Privacy Preserving Protocol for Cloud-Based Vehicular DTNs

Jun Zhou, Xiaolei Dong, Zhenfu Cao, Senior Member, IEEE, and Athanasios V. Vasilakos, Senior Member, IEEE

Abstract—Cloud-assisted vehicular delay tolerant networks (DTNs) have been utilized in wide-ranging applications where a continuous end-to-end connection is unavailable, the message transmission is fulfilled by the cooperation among vehicular nodes and follows a store-carry-and-forward manner, and the complex computational work can be delegated to the disengaged vehicles in the parking lots which constitute the potential vehicular cloud. Nevertheless, the existing incentive schemes as well as the packet forwarding protocols cannot well model continuous vehicle collaboration, resist vehicle compromise attacks and collusion attacks, leaving the privacy preservation issues untouched. In this paper, a novel threshold credit-based incentive mechanism (TCBI) is proposed based on the modified model of population dynamics to efficiently resist the node compromise attacks, stimulate the cooperation among intermediate nodes, maximize vehicular nodes’ interest, and realize the fairness of possessing the same opportunity of transmitting packets for credits. Then, a TCBI-based privacy-preserving packet forwarding protocol is proposed to solve the open problem of resisting layer-adding attack by outsourcing the privacy-preserving aggregated transmission evidence generation for multiple resource-constrained vehicles to the cloud side from performing any one-way trapdoor function only once. The vehicle privacy is well protected from both the cloud and transportation manager. Finally, formal security proof and the extensive simulation show the effectiveness of our proposed TCBI in resisting the sophisticated attacks and the efficiency in terms of high reliability, high delivery ratio, and low average delay in cloud-assisted vehicular DTNs.

Index Terms—Cloud computing, security and privacy, delay tolerant network, VANETs.

I. INTRODUCTION

DELAY tolerant networks (DTNs) have been recently increasingly applied to the applications such as distributed mobile healthcare systems and vehicular ad hoc networks (VANETs), where a contemporaneous end-to-end connection cannot be guaranteed [1]–[4]. Each selfish resource-constrained vehicle tries to cooperate in the energy-consuming task of message delivery, achieving the optimal reward by sacrificing the minimum cost [5]–[7]. Therefore, it is necessary to design an efficient incentive mechanism and packet forwarding protocol to stimulate the collaboration among vehicular DTN nodes.

During the past decades, cloud-assisted vehicular ad hoc networks, as a special case of DTNs, have greatly benefited to improving road safety and traffic efficiency. It mainly possesses the following unique characteristics [8], [11]. Firstly, though appropriately powered, Onboard Units (OBUs) storing private information for securing the communication in VANETs, equipped on the vehicles, are generally required to verify about 1000-5000 messages per second with about 100-500 vehicles in the communication range and unable to afford computational tasks with heavy complexity, and tempted to suffer from sophisticated attacks and even node compromise attack [12]. Additionally, the disengaged vehicles in the parking lots with considerably spare computational ability can constitute the distributed vehicular cloud for delay tolerant networks (CV-DTNs). They can perform the outsourced computation delegated from active (running) vehicles such as calculating, reporting and disseminating the average driving velocities in the main streets to efficiently decide controlling strategies, determine driving routes for vehicles and avoid terrible traffic jams. Last but not least, both the distributed semi-trusted vehicular cloud and other malicious active vehicles (i.e. or the collusion of them) try to extract from the interactions with the honest vehicles the useful private information such as the vehicle’s identity, location, driving velocity, direction and routings in CV-DTNs. Therefore, except for the traditional security requirements such as data confidentiality and authentication, unique security and privacy issues are emergently required to be solved. According to the observations mentioned above, in this paper, a threshold incentive scheme (TCBI) and the corresponding secure and reliable data forwarding scheme in CV-DTNs are proposed. The main contributions of the paper can be described as follows.
Firstly, due to the high moving velocity and the essence of intermittent routing of vehicular DTNs, once a selected routing is blocked (i.e. one of the intermediate vehicular node could not successfully find a successive node at the next hop for message forwarding in a specified time period, the message would be dropped with a high probability.), the routings in VANETs are occasionally required to be re-established, which is so energy-consuming that it is out of the resource-constrained vehicular nodes’ tolerance. On the other hand, due to the possibility of OBU compromise, if one of the intermediate vehicular nodes in the selected routing were compromised, the transmitted message would be absolutely exposed. To enhance both the data confidentiality and reliability, a \((t,n)\) threshold credit-based incentive scheme (TCBI) is proposed. The message is divided into \(n\) packet shares and transmitted respectively. If no less than \(t\) packet shares associated to the message are delivered, the original message would be successfully recovered.

Secondly, TCBI is proposed to prevent packet forwarding in CV-DTNs from node compromise attacks and efficiently stimulate the cooperation among the selfish vehicular nodes. It is likely for the intermediate nodes to attract more packets from its predecessors to earn more credits even by sponsoring sophisticated attacks such as sybil attacks or crowding at the hotspots (downtown) where the packet transmission is frequently requested (i.e. leaving the packet transmission requests in the suburb always neglected). However, the adversary can detect the intermediate nodes which have received more packets than others by monitoring the traffic flows in the whole network and/or analyzing the energy emission from the vehicular nodes. With setting these nodes as their attacking targets, more packets would be compromised by each attack and the probability of successfully recovering the message by the adversary as well as interrupting the message to be delivered to the destination would be significantly enhanced. In our proposed TCBI, the intermediate vehicular nodes are only rewarded when the message is successfully delivered and once the vehicular node is compromised, all the credits deposited in its credit account will be deleted. Therefore, the potentially existing node compromise attacks, on the other hand, will effectively impede the rational nodes from attracting more packets through illegal measures and the fairness of all the nodes possessing the same opportunity to transmit packets for credits can be realized. To solve the problems explained above, a novel threshold incentive mechanism TCBI is proposed based on the modified model of population dynamics. It can efficiently optimize the utility obtained by the intermediate vehicular nodes in the long run and simultaneously prevent the sophisticated attacks the rational nodes sponsored for maximizing their own interests.

Thirdly, based on TCBI and the multi-layered coin model, the proposed privacy-preserving packet forwarding scheme effectively solves the open problem proposed in [10] to resist the layer-adding attack by outsourcing the aggregated packet transmission evidence generation to the vehicular cloud from performing any one-way trapdoor function only once. The devised efficient privacy-preserving data aggregation guarantees individual vehicle user’s privacy to be well protected from both the semi-trusted cloud and the transportation manager.

Finally, formal security proof and extensive simulations illustrate the high practicability and efficiency of our proposed threshold credit-based incentive model TCBI and the corresponding packet forwarding scheme in terms of resisting node compromise attack, vehicle privacy preservation, high reliability, high delivery ratio and low average delay in CV-DTNs.

The remainder of this paper is organized as follows. In Section 2, we formalize the network architecture, the threat model, the preliminaries and our design goals. The threshold credit-based incentive mechanism (TCBI) is proposed in Section 3. Then, the TCBI-based data forwarding protocol is presented in Section 4, followed by the security analysis and performance evaluations in Section 5 and Section 6, respectively. We also review related works in Section 7. Finally, we draw our conclusions in Section 8.

II. MODELS AND PRELIMINARIES

In this section, we explain the network architecture, the threat model and the design goals of our proposed secure and privacy-preserving threshold incentive and data forwarding scheme TCBI in cloud-assisted vehicular DTNs.

A. Network Architecture

Cloud-assisted vehicular DTNs (CV-DTNs) are typically characterized by the unguaranteed continuous connectivity, low frequency of encounter between a specific pair of vehicular nodes, the distributed cloud server constituted by the RSUs appropriately deployed along the main streets and the clustering movement patterns. Fig. 1 illustrates the network architecture of the underlying CV-DTNs.

In CV-DTNs, vehicles are generally categorized into clusters since the ones in specific time and location are always moving with the same pattern such as the direction and velocity [1], [2]. Each vehicle is equipped with an Onboard Unit (OBU) allowing the mutual communication among different vehicular nodes under the 802.11p protocol [2]. Therefore, whenever two vehicles are moving into the transmission range of each other, they can exchange packets/bundles. However, the OBUs are generally resource-constrained, they can comply with the packet store-carry-and-forward pattern only when their storage is available. Otherwise, the packets would be...
straightforwardly dropped. Before transmitted, the message is divided into $n$ packets using $(t, n)$ threshold secret sharing scheme. Then, the source vehicle $S$ can deliver the packets through multiple distinct routings to the destination vehicle $D$ with the aid of data forwarding performed by the intermediate vehicular nodes. Different from OBUs, appropriately deployed RSUs are stationary and responsible for various tasks such as authenticating vehicle identities and monitoring the real-time traffic condition in the neighborhood. It also serves the access to the vehicular cloud which is composed of the disengaged vehicles in the distributed parking lots and their considerably spare computational ability constitutes a potential cloud for outsourced computation delegated by active vehicles or RSUs. Transportation manager (TM) generates the message transmission evidence for vehicles to justify their contribution to forwarding packet shares of specific messages. The accounting center (AC) takes on the tasks of verifying the authenticity of the transmission commitment aggregated by each intermediate vehicles using the evidence obtained from TM. If it passes verification, AC will perform the charging and rewarding according to the agreed payment strategies.

B. Threat Model

The resource-constrained OBUs equipped on vehicles are tended to be compromised and all the information stored in OBUs such as the private key for generating aggregated transmission commitment as well as the secret key agreed by the source and destination nodes for encrypting the message would be obtained from a compromised vehicle [3], [4]. The adversary can also sponsor eavesdropping, packet injecting, interruption and modification attacks. Especially in this paper, we identify a new kind of attack not considered in the existing work, namely targeting-oriented node compromise attack which is an upgraded version of node compromise attack since the adversary can select the nodes to compromise according to the observed network condition. In targeting-oriented node compromise attacks, the adversary possesses the ability to monitor the whole communication links and/or to meter the energy consumption in order for determining the potential target vehicle that received or sent the most data packets.

By compromising such vehicles, the adversary can obtain more packet shares and successfully recover the original message from one compromise attack with a significantly enhanced probability. Finally, it is assumed that there exists an efficient intrusion detection mechanism to estimate the whole network state such as the average compromise probability and execute revocation when a certain number of vehicles are compromised.

On the other hand, the distributed cloud servers composed by the disengaged vehicles in the parking lots are assumed to be semi-trusted (honest-but-curious) and they would comply with the protocol regulations but try their best to extract the private information such as the individual vehicle velocity and driving direction from the interactions with running vehicles. (i.e. the adversary can deduce some emergent incidences from an especially high driving velocity). Specifically in our proposed TCBI, since there exists a mutual authentication mechanism between the vehicles and their passing-by RSUs, the latter can be trusted and all vehicles’ realtime driving velocities are collected without being considered as a privacy issue. Therefore, the privacy preservation is required to be achieved for the semi-trusted vehicular cloud, the malicious running vehicles and even the collusion between them. The transportation manager (TM) is a government department, serves as a vehicular cloud client and takes responsibility of aggregating transportation information and generating the transmission evidence for vehicles. RSUs and TM are assumed to be fully trusted and would not arbitrarily modify their collected traffic data, fabricate the aggregated transmission evidence or collude with malicious vehicles. Finally, the accounting center is fully secure and trusted by all the vehicular nodes to fulfill the credit charging and rewarding tasks. In the following, we firstly define the formal security model of privacy preserving aggregated transmission evidence generation (ATEG) in our proposed TCBI. It is required that both the individual vehicle velocity and the average velocity of vehicle clusters should be well protected from the semi-trusted vehicular cloud and the malicious running vehicles.

1) Initialization Phase: On input $1^k$, the adversary queries a key generation oracle. The key generation oracle $O^{\text{Gen}}$ computes $(f, f^{-1}, G) \leftarrow_R AT EG.\text{Initialization}(1^k)$ on $G$ and gives back $pk_f$ to $A$ as the response.

2) Query Phase: The adversary $A$ makes polynomially-bounded number of queries to the decryption oracle $O^{\text{Dec}}$ and the random oracles $O^{H_2}, O^{H_5}$ at most $q_D, q_{h_4}, q_{h_5}$ times where $q_D + q_{h_4} + q_{h_5} \leq n(k)$ in total. The adversary respectively submits $c \in \mathbb{G}, q_{0}, q_{1} \in [0, 1]^*$ to $O^{\text{Dec}}$, $O^{H_2}$ and $O^{H_5}$, and receives $ATEG.\text{Dec}(1^k, sk_{fc}, c)$ and two random numbers $h_4, h_5 \in \mathbb{G}$ as the responses.

3) Challenge Phase: The adversary submits two messages $m_0, m_1 \in \mathbb{G}$ to the simulator, where $|m_0| = |m_1| = |\mathbb{G}|$. On input $m_0, m_1$, the simulator flips a coin and randomly selects $\beta \in_R \{0, 1\}$ and outputs $c^* \leftarrow_R AT EG.\text{Enc}(1^k, pk_f, m_\beta)$ as the challenge ciphertext to the adversary.

4) Adaptive Query Phase: The adversary continues to make queries to the decryption oracle $O^{\text{Dec}}$ and the random oracles $O^{H_2}, O^{H_5}$ with the restriction that the challenge ciphertext $c^*$ is not allowed to be submitted to $O^{\text{Dec}}$.

5) Guess Phase: The adversary outputs $\beta' \in \{0, 1\}$. If $\beta' = \beta$, we mean the adversary has successfully defeated the privacy preserving aggregated transmission evidence generation (ATEG) algorithm in our proposed TCBI.

Definition 1: Assume the CCA2 advantage of the adversary $A$ against the privacy preserving aggregated transmission evidence generation on the security parameter $k$ to be $Adv^{\text{CCA-ATEG}}_{A}(\lambda(k)) = |Pr[\beta' = \beta] - \frac{1}{2}|$ in the attack game described above. Then, we say our proposed privacy preserving aggregated transmission evidence generation algorithm is secure against adaptive chosen ciphertext attack if and only if for all probabilistic and polynomially-bounded adversary $A$ running in time at most $t$ and making totally at most $n(k)$ queries to the oracles $O^{\text{Dec}}$ and $O^{H_2}, O^{H_5}$.

\[
Adv^{\text{CCA-ATEG}}_{A}(\lambda(k)) \leq \epsilon(k),
\]

where $\epsilon(k)$ is a negligible function in $k$. 

Then, we can derive the security definition of our proposed TCBI against the layer-adding attack which refers to colluding malicious vehicles are intended to detour the packet forwarding path from the source to the destination for increased credits.

Definition 2: Assume the CCA2 advantage of the adversary $A$ against our proposed privacy preserving aggregated transmission evidence generation is $\text{Adv}_{\text{CCA}^{\text{ATEG}}_{\text{A}(\text{0}, k)}(k)}$ and the probability that $A$ successfully outputs a forgery in the exploited identity-based sequential aggregate signature [13] is $\text{Adv}_{\text{U}$-$\text{IBSAS}}_{\text{A}(\text{0}, q_k, q_h, \text{q}_{\text{th}}, \text{q}_{\text{kk}}, \text{q}_t)}(k)$. Then, we say our proposed TCBI is secure against layer-adding attack if and only if for all probabilistic and polynomially-bounded adversary $A$ running in time at most $t$ and making totally at most $n(k)$ queries to the oracles $O^{\text{Dec}}$ and $O^{\text{H}_i}, O^{\text{H}_s}, \text{q}_b, \text{q}_h, \text{q}_t$, queries to its hash oracles, its key-derivation oracle and its signing oracle with $n(k)$ as the maximal length of the output lists,

$$\text{Adv}_{\text{LayADD}}_{\text{TCBI}}(k) = \text{Adv}_{\text{CCA}^{\text{ATEG}}_{\text{A}(\text{0}, k)}(k)} + \text{Adv}_{\text{U}$-$\text{IBSAS}}_{\text{A}(\text{0}, q_k, q_h, \text{q}_{\text{th}}, \text{q}_{\text{kk}}, \text{q}_t)}(k) \leq \epsilon(k),$$

where $\epsilon(k)$ is a negligible function in $k$.

C. Preliminaries

1) Bilinear Maps [14]: Let $G$ be a cyclic additive group and $G_T$ be a cyclic multiplicative group of the same order $p$. Let $g, g_T$ respectively be the generators of group $G$ and $G_T$. We further assume that $e: G \times G \rightarrow G_T$ is an efficiently computational map with the following three properties:
(a) Bilinearity: For any $u, v \in G$ and $a, b \in Z$, we have $e(u^a, v^b) = e(u, v)^{ab}$.
(b) Non-degeneracy: For any generator $g \in G$, we have $e(g, g) \neq 1_{G_T}$.
(c) Computability: For any $u, v \in G$, there is an efficient algorithm to compute $e(u, v)$.

It is observed that the bilinear map $e(\cdot, \cdot)$ is symmetric since $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

2) One-Way Trapdoor Function [15]: A one-way trapdoor function generator is a probabilistic polynomial time (PPT) algorithm $G(1^k)$ (i.e. $k$ is the security parameter) which outputs a triple of functions $(f, f^{-1}, d)$. The former two are deterministic and the latter is probabilistic. It is required that $\{d(1^k)\}$ be subset of $[0, 1]^k$ and that $f, f^{-1}$ to be functions on $\{d(1^k)\}$ that are inverses of each other, where the notation $[X]$ refers to the support (i.e. the set of elements with positive probability) of $X$ distributed over a probability space. For all probabilistic polynomial time adversary $A$, $e(k) = \Pr((f, f^{-1}, d) \leftarrow G(1^k))$; $x \leftarrow d(1^k); y \leftarrow f(x) : A(f, d, y) = x$ is negligible in $k$, where $f, f^{-1}, d$ are all computable in polynomial time $t(k)$.

3) IBSAS-CDH Problem [13]: The IBSAS-CDH problem is a CDH-type problem defined as follows. Fix a bilinear group generator $G$. For $(p, G, G_T, e)$ output by $G$, we define for all $a_1, b_1, a_2, b_2 \in Z_p$ and $g \in G$ the associated oracle $O^{\text{IBSAS}$-$\text{CDH}}_{g, a_1, a_2, b_1, b_2}(\cdot)$ taking as input $m \in Z_p$ and defined as $O^{\text{IBSAS}$-$\text{CDH}}_{g, a_1, a_2, b_1, b_2}(m) : r, x \leftarrow Z_p$, $\text{Return}(g^{r^2} g^{a_1b_1}, g^{a_2b_2}, g', g'')$. We then define the IBSAS-CDH-advantage of an algorithm $A$ relative to $G$ as $\text{Adv}^{\text{IBSAS}$-$\text{CDH}}_{G}(A) = \Pr[C = (m', g', g'' \leftarrow g^{a_1b_1}, g^{a_2b_2}, g', g'') : (p, G, G_T, e) \leftarrow G; g \leftarrow G; a_1, a_2, b_1, b_2 \leftarrow Z_p; C \leftarrow \{g^{a_1b_1}, g^{a_2b_2}, g', g''\}]$, where it is required that $m' \in Z_p$ was not queried by $A$ to its oracle. The computational hardness of IBSAS-CDH problem has been formally proved in [13].

III. THRESHOLD CREDIT-BASED INCENTIVE MECHANISM TCBI

In our proposed TCBI, it is assumed that $\theta$ credits are rewarded for transmitting a packet of fixed size per unit distance. The last intermediate vehicle submits the aggregated packet transmission commitment to the accounting center and the accounting center charges the source vehicular node for the message delivery if it is successfully recovered at the destination as suggested in [9]. On the other hand, the intermediate nodes would be rewarded only for transmitting the first $t$-arriving packet shares utilized to successfully recover the message. The reason is that in our proposed (t,n) threshold credit-based incentive mechanism TCBI, it is required for the destination to use the firstly obtained $t$ packets to recover the corresponding message. For the later arriving $n-t$ packets, they would be useless and dropped by the destination.

Different from the fairness of charging both the source and destination nodes in [10], the fairness in TCBI lies in the equal opportunity for each intermediate node to transmit packets for earning credits. The fact is that, in addition to the reliability achieved in our threshold credit-based incentive mechanism, each intermediate node will carefully judge how many packets it accepts for transmission. Undeniably, the more packets one intermediate node transmits, the more credits it will be rewarded. However, simultaneously the higher the probability of being selected as the target of compromise attack will be. Once the intermediate node is compromised, all the packets stored in it will be exposed, interrupted or modified by the adversary and the opportunity of transmitting packets for credits will be deprived by the accounting center. Therefore, it becomes a two-edged sword and a critical task for the intermediate vehicular nodes to determine the number of transmitted packets.

To achieve the optimal utility equilibrium between transmitting packets for credits and resisting targeting-oriented node compromise attack, the modified model of population dynamics is proposed in our TCBI. The useful notations are illustrated in Table 1. In this paper, for briefly explaining the threshold credit-based incentive mechanism TCBI, we only consider the situation of $n$ packet shares associated to one specific message and it can be straightforwardly extended into the scenario of multi-message delivery.

The credits rewarded to each intermediate vehicular node can be calculated as $C_i = \theta s_i^{\text{eqm}} |L_i - L_{i-1}|$, (2)
where \( \theta, x_i^{eqm}, L_{i-1}, L_i \) respectively refers to the unit credit reward, the number of transmitted packets, the starting location and the ending location of the intermediate vehicular node \( i \). For fixed \( \theta \) and \( D_i \), where \( D_i = |L_i - L_{i-1}| \), the credit increasing ratio \( \frac{\Delta C_i}{dC_i/dt} \) (i.e. the credits earned by vehicular node \( i \) per unit time period) can be measured by the packet increasing ratio \( \frac{\Delta n_i}{dC_i/dt} \) of each intermediate node. For the two intermediate nodes competing for transmitting packets, the packet increasing ratios can be denoted respectively as follows,

\[
\begin{align*}
\frac{dx_1}{dt} &= r x_1 (1 - \frac{p x_2 + (x_1 - p x_2) r_0}{n}) \\
\frac{dx_2}{dt} &= r x_2 (1 - \frac{q x_1 + (x_2 - q x_1) r_0}{n})
\end{align*}
\]

(3a) (3b)

where \( p = \mu_2 \beta, q = \mu_1 \beta \) and \( \beta, \mu_1, \mu_2 \) respectively refer to the average selfish ratio all over the underlying CV-DTNs and the selfish coefficients of vehicle 1 and vehicle 2. It is noted that the higher the selfish coefficient is, the more packets the corresponding vehicle wants to seize from others.

**Theorem 1:** When \( P_{reqm} = p = q, r > 0, r_0 < \frac{Pr_{eqm}}{1 + Pr_{eqm}} \left( \frac{n}{r_0}, \frac{n}{r_0} \right) \) results in the required equilibrium in our proposed TCBI.

**Proof:** To find the equilibrium of the proposed threshold credit-based incentive mechanism TCBI, we firstly solve the following equations to find the singular points of equations (2a) and (2b).

\[
\begin{align*}
f_1 &= r x_1 (1 - \frac{p x_2 + (x_1 - p x_2) r_0}{n}) = 0 \\
f_2 &= r x_2 (1 - \frac{q x_1 + (x_2 - q x_1) r_0}{n}) = 0
\end{align*}
\]

(4a) (4b)

Then, we can obtain the following four singular points

\[
\begin{align*}
P_1 &: (0, 0), \quad P_2 : (0, \frac{n}{r_0}), \quad P_3 : (\frac{n}{r_0}, 0), \quad P_4 : (\frac{n}{r_0}, \frac{n}{r_0} - \frac{n r_0 + r_0 q - q}{n r_0 + r_0 q - q})
\end{align*}
\]

Now, we give the derivation of the functions \( f_1, f_2 \) in equations (3a) and (3b).

\[
\begin{align*}
a_1 &= \frac{df_1}{dx_1} = r (1 - \frac{p x_2 + (x_1 - p x_2) r_0}{n}) - \frac{r x_1 r_0}{n} \\
a_2 &= \frac{df_2}{dx_2} = -r x_1 (p - r_0 p) \\
b_1 &= \frac{df_1}{dx_1} = -r x_2 (q - r_0 q) \\
b_2 &= \frac{df_2}{dx_2} = r (1 - \frac{q x_1 + (x_2 - q x_1) r_0}{n}) - \frac{r x_2 r_0}{n}
\end{align*}
\]

For \( P_1 : (0, 0), \)

\[
a_1 = r, a_2 = 0, b_1 = 0, b_2 = r
\]

(5)

The associated characteristic equation is \( (r - \lambda)^2 = 0 \) possessing the roots \( \lambda_1 = \lambda_2 = r \). When \( r < r_0 - r_d < 0 \), namely the average packet dropping rate is no less than the average packet generation rate, the equilibrium is achieved. In this case, no packets can be successfully delivered to the destination and no credits will be rewarded to the intermediate vehicular nodes. Therefore, it is not the outcome we want and cannot be applied to the vehicular DTNs.

For \( P_2 : (0, \frac{n}{r_0}), \)

\[
a_1 = r (1 - \frac{p}{r_0}), \quad a_2 = 0, \quad b_1 = \frac{-r (q - r_0 q)}{r_0}, \quad b_2 = -r
\]

(6)

The associated characteristic equation is

\[
(r (1 - \frac{p}{r_0}) - \lambda) (-r - \lambda) = 0
\]

(7)

possessing the roots \( \lambda_1 = r (1 - \frac{pm}{n + n m}), \lambda_2 = -r \). To achieve equilibrium, it is required that \( r > 0 \) and \( p (1 - r_0) > r_0 \).

It means when the following two conditions are simultaneously satisfied, namely (a) the average packet generation rate is higher than its average dropping rate and (b) the number of the packets seized by vehicle 2 from vehicle 1 is more than the packets the adversary compromises from vehicle 1, the equilibrium would be achieved. In this case, vehicle 1 secures from packet transmitting and the equilibrium is only achieved between vehicle 2 and the adversary. Therefore, this outcome is also inappropriate to the underlying vehicular DTNs. For \( P_3 : (\frac{n}{r_0}, 0), \) the other equilibrium as the counterpart of \( P_2 \) can be straightforwardly derived when \( q (1 - r_0) > r_0 \) namely the number of the packets seized by vehicle 2 from vehicle 1 is more than the compensated packets from vehicle 2. As a result, this equilibrium still cannot satisfy the requirement of our proposed threshold incentive scheme TCBI.

For

\[
P_4 : \left( \frac{n r_0 + r_0 p - p}{r_0^2 - pq + 2 pr_0 q - r_0 q^2}, \frac{n r_0 + r_0 q - q}{r_0^2 - pq + 2 pr_0 q - r_0 q^2} \right)
\]

The associated characteristic equation is

\[
(a_1 - \lambda) (b_2 - \lambda) - a_1 b_2 = 0
\]

(8)

where \( a_1, a_2, b_1, b_2 \) are shown at the bottom of the next page. The corresponding characteristic roots are

\[
\begin{align*}
\lambda_1 &= -r \\
\lambda_2 &= \frac{r (r_0 q - r_0 q + r_0^2 p - r_0 q + r_0^2 p - r_0 q + r_0^2 p)}{r_0^2 - pq + 2 pr_0 q - r_0 q^2}
\end{align*}
\]

Without loss of generality, it is assumed that \( 0 < p < q < 1 \). Therefore, to achieve equilibrium, either of the following conditions should be satisfied, (a) \( r > 0, r_0 < \frac{p}{1 + q} \) (b) \( r > 0, r_0 > \frac{p}{1 + q} \). From condition (b), we can derive that \( r > 0, r_0 > q (1 - r_0) > p (1 - r_0) \), which means the number of packets compromised by the adversary is more than the packets the vehicular nodes seizes from each other. Since one

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( r_g )</td>
<td>Average packet generation rate in the VANETs</td>
</tr>
<tr>
<td>( r_d )</td>
<td>Average packet dropping rate in the VANETs</td>
</tr>
<tr>
<td>( r )</td>
<td>( r_g - r_d ) Average packet availability rate in the VANETs</td>
</tr>
<tr>
<td>( x_i )</td>
<td>Original number of packets owned by vehicle ( i )</td>
</tr>
<tr>
<td>( p )</td>
<td>Probability of the packets seized from vehicle 1 by vehicle 2</td>
</tr>
<tr>
<td>( q )</td>
<td>Probability of the packets seized from vehicle 2 by vehicle 1</td>
</tr>
<tr>
<td>( r_0 )</td>
<td>Probability of vehicle compromise (Adversary’s ability)</td>
</tr>
<tr>
<td>( n )</td>
<td>Total number of packets associated to one specific message</td>
</tr>
</tbody>
</table>

| TABLE I |

<table>
<thead>
<tr>
<th>Notations in Our Proposed Threshold Incentive Mechanism TCBI</th>
</tr>
</thead>
<tbody>
<tr>
<td>( r_g )</td>
</tr>
<tr>
<td>( r_d )</td>
</tr>
<tr>
<td>( r )</td>
</tr>
<tr>
<td>( x_i )</td>
</tr>
<tr>
<td>( p )</td>
</tr>
<tr>
<td>( q )</td>
</tr>
<tr>
<td>( r_0 )</td>
</tr>
<tr>
<td>( n )</td>
</tr>
</tbody>
</table>
of the purposes of our proposed TCBI is to efficiently resist node compromise attack, this equilibrium would be discarded. On the other hand, we can derive from condition (a) that \( r > 0, r_0 < p(1 - r_0) < q(1 - r_0) \), which means the number of packets compromised by the adversary is less than the packets the vehicular node seizes from each other. In addition to the other requirement that the average packet generation rate is higher than its average dropping rate, the equilibrium can be achieved. The vice is versa. Especially when \( P_{eqm} = p = q \), we can conclude that when \( r > 0, r_0 < \frac{r}{1 + P_{eqm}} \), each intermediate vehicular node transmits equal number of packets \( N_{eqm} = \frac{m(P_{eqm} - r_0 P_{eqm} - r_0)}{(P_{eqm} - 1) r_0 - 2 P_{eqm} r_0 + P_{eqm}} \) for earning credits. Without loss of generality, from condition (a), let \( P_{eqm} = p \) and we can derive that \( N_{eqm} = \frac{n}{r_0 - (r_0 - 1)p} \) and \( p > \frac{r_0}{1 - r_0} \). It is observed that when \( n \) and \( r_0 \) are fixed, \( N_{eqm} \) increases as \( p \) decreases. Therefore, when \( p = \frac{r_0}{1 - r_0} \), we derive that the transmitted number of packets in the equilibrium is \( N_{eqm} = \frac{n}{r_0} \). In this case, the vehicular nodes cooperate to optimize the number of each other’s transmitted packets (i.e. as well as the associated credit rewarding) and on the meanwhile, efficiently resist the node compromise attack. The equilibrium in this case well adapts to the requirements of the underlying threshold incentive scheme TCBI in vehicular DTNs. This completes the proof.

IV. THE PROPOSED TCBI-BASED DATA FORWARDING SCHEME

In this section, we give a detailed presentation of our proposed efficient privacy-preserving TCBI-based data forwarding scheme in CV-DTNs which comprises the following four phases: System Initialization, Vehicle Clustering, Bundle Generation, Bundle Forwarding and Aggregated Transmission Evidence Generation, Charging and Rewarding.

A. Multi-Layered Coin Model

It is required for us to secure the underlying threshold incentive mechanism TCBI to guarantee it working well. Therefore, we utilize the multi-layered coin to stimulate the bundle delivery [9], [10]. A typical multi-layered coin model is composed of a base layer constructed by the source vehicular node and multiple endorsed layers constructed by the intermediate vehicular nodes. Fig. 2 illustrates the structure of the multi-layered coin architecture. In the base layer \( BL, S \), \( LS \) and \( D, LD \) respectively represents the identities and the locations of the source vehicle and the destination vehicle. \( TCBI \) suggests the underlying threshold incentive mechanism including the charging and rewarding policy. \( TS_5, TTL \) refers to the time stamp and the time-to-live information. \( MsgID \) denotes the identifier of the message, to which the associated packet share belongs. \( Index_k \) refers to the index of the \( k \)-th packet share w.r.t. one specific message \( MsgID \) in our \((t, n)\) threshold credit-based secure data forwarding scheme. \( N_i \) is the first intermediate vehicular node transmitting the packet. \( Sig_{S_i}, Sig_{S_i,N_i} \) denotes the commitment made by the source node showing that it indeed sponsored the bundle transmission and would be charged afterwards. In the endorsed layer \( i \), \( N_i, L_i \) refers to the identity of the \( i \)-th intermediate node and its location. \( N_i+1 \) refers to the subsequent intermediate vehicle forwarding the packet. \( Sig_i^{agg} \) is the aggregated transmitting witness of the intermediate vehicular nodes showing their cooperation in relaying the packets and will be submitted to the accounting center for clearance if their transmitted packets belong to the first \( t \) arriving shares and are utilized to successfully recover the original message, preventing malicious nodes from disrupting the system.

B. TCBI

Based on the proposed threshold credit-based incentive mechanism TCBI and the multi-layered coin model, a secure and efficient privacy-preserving packet forwarding scheme is proposed in this subsection. It effectively solves the open

\[
\begin{align*}
\begin{array}{l}
a_1 = r \left(\frac{1}{n} - \frac{-p(-q + r_0 q + r_0)}{r_0 + pq - 2 pr_0 q + r_0^2 p q} \right) + \frac{-r_0 (r_0 + r_0 p - p)}{r_0 r_0 (r_0 + r_0 p - p)} + \frac{r_0 p (-q + r_0 q + r_0)}{r_0 q + r_0 p + r_0^2 q + r_0^2 p q}
\end{array}
\end{align*}
\]

\[
\begin{align*}
\begin{array}{l}
a_2 = \left\{ \begin{array}{l}
-\frac{r_0 + pq - 2 pr_0 q + r_0^2 p q}{r_0 + r_0 p - p (p - r_0)} \\
-\frac{r_0 + pq - 2 pr_0 q + r_0^2 p q}{r_0 + r_0 p - q (q - r_0)}
\end{array} \right.
\end{array}
\end{align*}
\]

\[
\begin{align*}
\begin{array}{l}
b_1 = \frac{1}{n} \left( -\frac{q (-p + r_0 p + r_0)}{r_0 + pq - 2 pr_0 q + r_0^2 p q} \right) + \frac{-r_0 (r_0 + r_0 q - q)}{r_0 (r_0 + r_0 q - q)} + \frac{r_0 q (-p + r_0 p + r_0)}{r_0 q + r_0 p + r_0^2 q + r_0^2 p q}
\end{array}
\end{align*}
\]

\[
\begin{align*}
\begin{array}{l}
b_2 = \frac{1}{n} \left( -\frac{-q (-p + r_0 p + r_0)}{r_0 + pq - 2 pr_0 q + r_0^2 p q} \right) + \frac{-r_0 (r_0 + r_0 q - q)}{r_0 (r_0 + r_0 q - q)} + \frac{r_0 q (-p + r_0 p + r_0)}{r_0 q + r_0 p + r_0^2 q + r_0^2 p q}
\end{array}
\end{align*}
\]
problem proposed in [10] to resist the layer-adding attack by exploiting the technique of identity-based sequential aggregate signature [13] and designing the outsourced aggregated packet transmission evidence generation to the vehicular cloud from performing any one-way trapdoor function.

1) System Initialization: We assume that all the vehicular DTN nodes \( N = \{N_1, N_2, \ldots, N_n\} \) and the accounting center \( AC \) possess the same system parameters. Given the security parameter \( k \), the bilinear parameters \((p, g, \mathbb{R}, \mathbb{R}_T, e)\) are first generated by running \( \text{Gen}(k) \) where \( p \) is a big prime and \( \mathbb{R}, \mathbb{R}_T \) are skew fields with the multiplicative groups of order \( p \). \( g \) is the generator of the multiplicative group of \( \mathbb{R} \) and \( e : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}_T \) is the bilinear mapping on the corresponding multiplicative groups of \( \mathbb{R} \) and \( \mathbb{R}_T \). Then, the algorithm randomly chooses \( a_1, a_2 \in \mathbb{R}_p \) and cryptographic hash functions \( H_0, H_1, H_2, H_A, H_S : \{0, 1\}^* \rightarrow \mathbb{R} \) and \( H_3 : \{0, 1\}^* \rightarrow \mathbb{Z}_p^* \). Finally, the system runs a one-way trapdoor function generator denoted as a PPT algorithm \( \mathcal{G}(k) \) and outputs \((f, f^{-1}, f_1, f_1^{-1}, f_s, f_s^{-1})^{-1}(i = 1, 2, \ldots, n)\) with the public keys \( PK_{f_i}, PK_{f_s}, PK_{f_f}, f_{i, f} \) and the secret keys \( SK_{f_i}, SK_{f_s}, SK_{f_f} \) associated to the transportation manager, each vehicle \( i \) and the system. It returns \((\mathbb{R}, \mathbb{R}_T, e, f, PK_{f_i}, g, g^{a_1}, g^{a_2}, H_1, H_2, H_3)\) as the public parameters and the \((a_1, a_2)\) as the master secret key. Each vehicle submits its unique identity \( N_i \in \{0, 1\}^* \) to the PKG, and it returns \((H_1(N_i)^{a_1}, H_2(N_i)^{a_2})\) as the private key. After registering at the accounting center, each vehicle possesses a personal credit account for charging and rewarding.

2) Vehicle Clustering: Initially, \( K \) points are randomly selected as cluster centers by the system, according to the vehicle geographical distribution and social spot deployment. Then, \( n \) vehicles can be dynamically categorized into \( K \) independent clusters with location privacy preservation as follows. Let \((L_{i,x}, L_{i,y})(i = 1, 2, \ldots, n)\) be the horizontal and vertical components of the location for vehicle \( i \), and \((L_{c,x}, L_{c,y})(c = 1, 2, \ldots, K)\) be locations of cluster centers, where \( L_{m,i} \in \mathbb{R}(m \in \{0,1\}, l \in \{x,y\}) \). Each vehicle \( i \) randomly selects \( r_i \in \mathbb{R}_p \), computes \( C_{1,i} = f_s(r_i), C_{2,i} = \text{Dist}_{i,c}^{\text{bld}} = r_i((L_{i,x} - L_{c,x})^2 + (L_{i,y} - L_{c,y})^2), C_{3,i} = H_0(r_i \parallel C_{2,i}), C_{4,i} = \text{Dist}_{i,c}^{\text{bld}} \) using \( PK_{f_i} \) and transmits \((C_{1,i}, C_{2,i}, C_{3,i}, C_{4,i})\) to the system (TM). Then, TM deciphers \( r_i \) using \( SK_{f_i} \), checks whether \((C_{3,i} = H_0(r_i \parallel C_{2,i})\) holds, and recovers the original distances between vehicle \( i \) and each cluster centers by computing \( \text{Dist}_{i,c} = r_i^{-1} \text{Dist}_{i,c}^{\text{bld}} \). For each cluster \( c, TM \) selects the vehicle \( i \) with \( \text{Min}(\text{Dist}_{i,c})(i = 1, 2, \ldots, n) \) as the cluster head, and categorizes each vehicle \( i \) of the left \( n-K \) vehicles to cluster \( c \) with \( \text{Min}(\text{Dist}_{i,c})(c = 1, 2, \ldots, K) \). After cluster initialization, vehicle clustering would be updated dynamically as vehicles are continuously moving, which resembles the cluster initialization phase with the exceptions that the updating is charged by the cluster head and the blinding factor \( r_i \) is required to be encoded in \( f_s \) assigned to vehicle \( c \) as the cluster head of cluster \( c \). It is noted that only the authorized TM and the cluster heads, respectively holding the secret keys of \( f_s \) and \( f_c \) can successfully decipher \( r_i \) to recover the distances between each vehicle and the cluster centers(heads). \( f_s, f_c \) can be implemented by kinds of public key encryptions, such as RSA, identity-based encryption and attribute-based encryption, according to different security and privacy requirements in distinguished network scenarios. The precise vehicle location privacy can be well protected, since even TM and the cluster heads can only know the vehicle is located at a circle with its center at TM/cluster heads and of radius the recovered distance.

3) Bundle Generation: When the source vehicle \( S \) wants to transmit a bundle to the destination vehicle \( D \), it firstly computes the shared symmetric key as \( K = e(H_1(D), H_1(S)^{a_1}) \) between \( S \) and \( D \) and encrypts the bundle \( m \) using \( K \) under the shared symmetric encryption scheme \( B = E_K(m) \). After that, the source node \( S \) randomly selects a \( t \) of \( 1 \)-degree polynomial \( f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1} \) with the coefficients \( a_0, a_1, \ldots, a_{t-1} \in \mathbb{R} \) and sets \( a_0 = B \) as the secret. Then, by exploiting Shamir’s secret sharing technique, \( S \) can generate \( n \) shares of \( B \) as the packets \( PACK = \{P_1, P_2, \ldots, P_n\} \) prepared for transmission and for each packet, \( S \) signs on the bundles as follows.

3.a) Before transmitting the data packet \( P_k \) associated to message identifier \( MsgID \), the source vehicle \( S \) (i.e. the same operations are performed by the intermediate vehicles at the \( i \)-th hop \((i = 1, \ldots, w)\) forwarding packets) broadcasts the packet sending commitment \( \text{Sig}_S = H_1(S)^{a_1}H_t(P_k||\text{Info}_S) \), where \( \text{Info}_S = S || L_s || D || L_D || TCBI || TTL || MsgID || \text{Index}_k \).

3.b) It is assumed that there exist \( n_1 \) candidates at the first hop, denoted as \( N_{1,k}(k = 1, \ldots, n_1) \), are interested in the bundle forwarding. It firstly checks whether its total number of packets in the store-carry-and-forward mode exceeds \( \frac{n_1}{\alpha^2} \) in the equilibrium derived in Sec. 3. If not, it verifies the source vehicle \( S \)’s packet sending commitment \( \text{Sig}_S \) by checking whether \( e(\text{Sig}_S, g) = e(H_1(S)^{a_1}H_t(P_k||\text{Info}_S), g^{a_1}) \) holds. It passes authentication, \( N_{1,k} \) generates the packet transmitting response \( \text{Sig}_{N_{1,k}} = H_1(N_{1,k})^{a_1}H_t(P_k||\text{TS}_S||S||\text{Index}_k) \) and sends it back to \( S \). Without loss of generality, let \( N_{1,1} \) be the vehicle whose packet transmitting response \( \text{Sig}_{N_{1,1}} \) is firstly received by \( S \). Then, \( S \) checks whether \( N_{1,1} \) has transmitted more than a pre-defined threshold number \( t' < \frac{n_1}{\alpha^2} \) \( (i.e. t' \) is the threshold in the secret sharing scheme) data packets associated to one specific message \( MsgID \). (i.e. the selection of \( t' \) is evaluated in Fig. 9(c) of Sec. 6.2.)

3.6.1 If not, \( S \) checks the time stamp and verifies the packet transmitting response \( \text{Sig}_{N_{1,1}} \) by checking whether \( e(\text{Sig}_{N_{1,1}}, g) = e(H_1(N_{1,1})^{a_1}H_t(P_k||\text{TS}_S||S||\text{Index}_k), g^{a_1}) \) holds; otherwise, it executes step (3.6.3).

3.6.2 If it passes verification, \( S \) generates the packet transmitting commitment for \( N_{1,1} \), denoted as \( N_1 \), the finally-selected intermediate vehicle in the first hop

\[ \text{Sig}_{N_1} = H_1(S)^{a_1}H_t(P_k||\text{Info}_S||\text{TS}_S||S_1) \]
(3.b.3) $S$ selects $N_{1,k} (k = 2, \cdots, n_1)$ as the candidate for transmitting $P_k$ of $MsgID$ in the first hop, whose packet transmitting response $\text{Sig}_{N_{1,k}||S}$ is the $k$-th received. The following operations are the same as the ones for $N_{1,1}$ until the transmitter $N_1$ is finally selected. Finally, $S$ embeds the packet transmitting commitment $\text{Sig}_{S||N_1}$ into the base layer and sends the packet $P_k$ together with the base layer $BL$ to $N_1$.

4) Bundle Forwarding: When the intermediate vehicle $N_1$ receives $P_k$, $BL$ from the source vehicle $S$, it firstly checks the authenticity of the time stamp $TS_1$, verifies $BL$ by checking whether the packet is in its lifetime and verifies the packet transmitting commitment $\text{Sig}_{S||N_1}$ by checking whether $e(\text{Sig}_{S||N_1}, g) = e(H_1(S)H_3(P_k||\text{Info}_0||TS_1||N_1), g^a_1)$ holds. If it passes the verification, $N_1$ begins to forward the packet.

4.a) The packet $P_k$ is delivered to the destination vehicle $D$ by the opportunistic routing $S \rightarrow N_1 \rightarrow \cdots \rightarrow N_m \rightarrow D$. At location $L_i$, when the intermediate vehicle $N_i$ wants to forward $P_k$ to the subsequent vehicle, the following steps are performed. If the intermediate vehicle $N_{i+1}$ is interested in forwarding the packet, it firstly checks whether the total number of carried packets is less than $\frac{2}{\eta}$ derived in the equilibrium in Sec. 3. If it does, $N_{i+1}$ authenticates the multi-layered coin by checking whether the packet is in its lifetime and whether the linkage of multiple endorsed layers is preserved. Then, $N_{i+1}$ verifies the aggregated transmitting commitment $\text{Sig}_{agg}^{i+1}$ in the $i-1$-th endorsed layer by checking whether

$$e(\sigma_{i-1,1}, g) = e(\prod_{l=1}^{i-1} T_l(U_l)^{\bar{1}}, \sigma_{i-2,1}) e(\prod_{l=1}^{i-1} H_2(N_l), g^{a_2}) \prod_{l=1}^{i-1} H_1(N_l)^{H_3(N_l||P_k||\text{Info}_0||L_i||L_{i+1})}, g^{a_1}) \quad (12)$$

holds, where $\text{Info}_0 = P_k || BL || N_{i-1} || N_i || L_i || TS_i || Index_{k}$ (i.e. this step is skipped for the first intermediate vehicle, for which the aggregated transmitting commitment is $\text{Sig}_{agg}^{1} = (1_G, 1_G)$). If it passes authentication, $N_{i+1}$ signs

$$\text{Sig}_{N_{i+1}, N_i} = H_1(N_{i+1})^{\sigma_1} H_3(P_k||BL||TS_i||N_i||L_i||L_{i+1}) \quad (13)$$

and sends it back to $N_i$.

4.b) $N_i$ checks the time stamp and verifies the validity of $\text{Sig}_{N_{i+1}, N_i}$ by checking $e(\text{Sig}_{N_{i+1}, N_i}, g) = e(H_1(N_{i+1})H_3(P_k||BL||TS_i||N_i||L_i||L_{i+1}), g^{a_1})$. If it is valid, $N_i$ firstly computes the time period to which it belongs by calculating $PER_i = \frac{T_S - TS_i}{\Delta T}$. The length of the time period $\Delta T$ is determined by the system, which should be carefully selected according to the adversary’s ability and the required security level. Then, $N_i$ generates the aggregated transmitting commitment as follows. It randomly selects $u_t, r_t, r_{l_t} \in Z_p$, computes

$$T_i = g^{t_i}, U_i = g^{u_i}, \sigma_{i,2} = \sigma_{i-1,2} g^{r_i},$$

$$X_i = (\sigma_{i,2})^{\gamma_i} PER_i^{m_i}, Y_i = (\prod_{j=1}^{i-1} T_j(U_j)^{\bar{1}})^{y_i}, \quad (14)$$

and

$$\sigma_{i,1} = \sigma_{i-1,1} X_i Y_i H_2(N_i)^{a_2} H_1(N_i)^{\gamma_i} H_3(N_i||P_k||\text{Info}_0||L_i||L_{i+1}), g^{a_1} \quad (15)$$

holds. If all of them pass verification, it then extracts the starting time stamp $TS_S$ and a series of location strings
StrLoc = Lₜ || L₁ || L₂ || ... || Lₜ || Lₜ

from BL, EL₁, EL₂, ..., ELₜ, ELₜ. Then, it generates the
signature $\text{Sig}_{\text{AC}} = \text{Sig}_{\text{BkAC}}(\text{Index}_k || TS_S || \text{StrLoc})$ and sends $\text{Index}_k, TS_S, \text{StrLoc}, \text{Sig}_{\text{AC}}$ to the transportation manager (TM) through the secure communication channel established between them [14]. For privacy consideration, the identities of the individual vehicles are not submitted for their tracing protection.

5.a) It is assumed that there exist $N_{c,T}^iTS_S$ vehicles belonging to the same cluster $c$ moving from location $L_S$ to $L_1$ at the time of $TS_S$ and $N_{S,1}$ RSUs deployed along the routing from $L_S$ to location $L_1$. TM firstly verifies the signature $\text{Sig}_{\text{AC}}$ received from the accounting center AC. If it passes verification, the velocity data $V_{L_S \rightarrow L_1, TS_S}$ ($i \in \{1, 2, \ldots, N_{c,T}^iTS_S\}, l \in \{1, 2, \ldots, N_{S,1}\}$) namely the velocity of the each vehicle $i$ belonging to the same cluster $c$, is monitored and collected by RSU $l$. Each of the RSUs performs the following operations to generate the privacy-preserving aggregated transmission evidence.

5.a.1) Each RSU $l$ randomly selects $r_1, r_1, l \in R$ and computes

$$C_{l,1} = f(r_1), C_{2,i} = V_{L_S \rightarrow L_1, TS_S}^{i,l} + r_i, l,$$

where $f(\cdot)$ is the underlying one-way trapdoor function on $R$ generated in System Initialization. It is assumed that there exist $N_{\ell}$ parking lots serving as distributed vehicular clouds in CV-DTNs. RSU $l$ respectively delegates $n_k$ encrypted individual vehicular velocities to vehicular cloud $k$ ($k \in \{1, 2, \ldots, N_{\ell}\}$) with the condition that $N_{c,T}^iTS_S = \sum_{k=1}^{N_{\ell}} n_k$. Then, RSU $l$ publicizes $r_{i,k}, T = \sum_{i=1}^{n_k} r_{i,k}, l$, computes $C_{k,ram} = H_4(r_1 || r_{i,k}, T)$ and sends $C_{l,k} = (ID_k, ID_k, C_{l,1}, C_{2,i}, C_{k,ram})(l \in \{1, 2, \ldots, n_k\})$ to vehicular cloud $k$ through the established authenticated communication channel [14], where $H_4 : [0, 1]^* \rightarrow R$ is the hash function.

5.a.2) When vehicular cloud $k$ receives $C_{l,k}$, it performs the data aggregation

$$C_{l,k,T} = \sum_{i=1}^{n_k} C_{l,2,i} = \sum_{i=1}^{n_k} V_{L_S \rightarrow L_1, TS_S}^{i,l} + \sum_{i=1}^{n_k} r_i, l$$

$$C_{3,k} = H_5(C_{l,k,T} || C_{k,ram}),$$

where $m_{k,l,T} = \sum_{i=1}^{n_k} V_{L_S \rightarrow L_1, TS_S}^{i,l}$, and sends $C_{l,k,agg} = (ID_k, ID_k, C_{l,1}, C_{l,k}, C_{k,ram}, C_{k,ram})$ to the transportation manager TM.

5.a.3) TM performs the decryption, computes the average velocity of the moving cluster $c$ and generates the aggregated transmission evidence as follows. Firstly, TM computes

$$r_i = f^{-1}(C_{l,1}), V_i, l = (\sum_{k=1}^{N_{\ell}} C_{l,k,T} - \sum_{i=1}^{n_k} C_{l,k,T}) r_i^{-1},$$

if both $C_{k,ram} = H_4(r_1 || r_{i,k}, T)$ and $C_{3,k} = H_5(C_{l,k,T} || C_{k,ram})$ hold; otherwise, it outputs $\bot$.

Then, TM calculates the average velocity of the vehicular cluster $c$ moving from location $L_S$ to location $L_1$ at time $TS_S$, the actual consuming time $T_{S,1}$ and the actual time period $PE_{T}^{\text{real}}$ the first intermediate vehicle belongs to as follows,

$$V_{L_S \rightarrow L_1, TS_S} = \frac{\sum_{i=1}^{N_{S,1}} V_{i, T}}{N_{S,1}N_{c,T}^iTS_S}, T_{S,1} = \frac{L_1 - L_S}{V_{L_S \rightarrow L_1, TS_S}}, PE_{T}^{\text{real}} = \left[\frac{T_{S,1}N_S}{\Delta T}\right],$$

For $L_2, \ldots, L_\ell$, TM calculates the $PE_{T}^{\text{real}}$ in the same way. It is noted that the one-way trapdoor function $f(\cdot)$ can be implemented by RSA, identity-based encryption or attribute-based encryption according to the different security and privacy requirements in various network applications.

5.b) TM generates the aggregated transmission evidences for packet transmitting through the routing $L_S \rightarrow L_1 \rightarrow \ldots \rightarrow L_\ell(L_D)$ as follows,

$$E_{\text{Evidence}_{L_1 \rightarrow L_{\ell+1}}} = \prod_{i=1}^{\ell} T_j(U_j)^{PE_{T}^{\text{real}}} (i = 1, 2, \ldots, w - 1),$$

on the evidences as $E_{\text{Sig}_{\text{TM}}} = E_{\text{Sig}_{\text{BkTM}}} (\{E_{\text{Evidence}_{L_1 \rightarrow L_{\ell+1}}}(i = 1, 2, \ldots, w - 1)\) and sends them with the associated signature to the accounting center AC.

5.c) AC firstly verifies the aggregated commitment $E_{\text{Sig}_{\text{w}}}^{\text{agg}}$ included in the $w$-th endorsed layer utilizing the transmission evidence $E_{\text{Evidence}_{L_1 \rightarrow L_{\ell+1}}}^{\text{agg}}$ as follows,

$$e(\sigma, 1, g) = e(E_{\text{Evidence}_{L_1 \rightarrow L_{\ell+1}}}, \sigma_{w,2}) e(\prod_{i=1}^{\ell} H_2(N_i), g^{\alpha_2}) e(\prod_{i=1}^{\ell} H_1(N_i)H_3(N_i||P_k||\text{Info}_0), g^\alpha_2).$$

(22)

If it passes the verification, all the intermediate vehicular nodes are proved to be honest in executing the threshold credit-based incentive mechanism TCBI.

5.d) AC checks whether these multi-layered coins have been deposited before by inquiring the source vehicle’s previous record and measures the number of valid packets delivered by each intermediate vehicle with their actual relay distances. Then, AC calculates the rewarding credits for each intermediate node according to the rewarding strategy explained in Eqn. (1), stores them into each vehicle’s personal credit account and charges the source vehicle by withdrawing the corresponding credits of transmitting the total of $n$ packet shares for reliability enhancement from its credit account. Specifically, if the source vehicle has successfully delivered message $m$ with identifier $MsgID$, the accounting center would firstly extract the layers including $MsgID$ and $\text{Index}_k$ from the multi-layered coin model submitted by the last intermediate vehicle $N_k$ for the firstly arriving $t$ packet shares, and from the transmitting commitments $E_{\text{Sig}_{S,N}} = H_4(S)||H_5(R_k||\text{Info}_0||TS_S||N_k)(k = 1, \ldots, n)$, received from the source vehicle $S$ by the intermediate vehicles $N_k$ for the left $n - t$ shares, which cannot be denied by the source vehicle $S$. Then, the total number of transmitted packet shares $n$ can be decided, and AC charges the source vehicle according to Eqn. (1). The extra credit charged from the source vehicle...
S for enhancing delivery reliability by transmitting n packet shares could be used to afford the outsourced computation performed by the vehicular cloud in a pay-per-use manner to generate the aggregated transmission evidence.

V. Security Analysis

In this section, we discuss the security of our proposed TCBI from the following aspects: the fairness vs. the targeting-oriented node compromise attack, the free riding attack, the layer-removing/adding attack and the privacy-preserving aggregated transmission evidence generation. Since it is assumed that all the vehicular nodes are rational, we focus on the attacks sponsored by the selfish nodes.

A. Fairness vs. Targeting-Oriented Node Compromise Attack

The incentive policy in the proposed TCBI is fair to both the source vehicle and the intermediate vehicles. It is necessary to charge the source vehicle for sending all n packets associated to one specific message m when they are successfully delivered, since the redundant packet shares are transmitted for reliability enhancement. On the other hand, only the intermediate vehicles transmitting the first t arriving packets successfully used in recovering the message m can be rewarded, which can be undeniably guaranteed by the aggregated packet transmitting commitment. For fairness consideration, the design of only rewarding the vehicles transmitting the first t-arriving packet shares effectively stimulates the selfish vehicles to deliver packets to the destination timely and prevents them from crowding among hot social spots where more packets are generated and disseminated. More seriously, if the overdue n − t packet share transmission were rewarded, the selfish vehicles (or the adversary) would deliberately detour the packet transmission route to swindle more credits.

Especially in our proposed TCBI, the fairness is also manifested in sharing the equal opportunity of forwarding packets for earning credits among all the vehicles. By proposing an improved model of population dynamics in TCBI, the conflict between packet forwarding and resisting targeting-oriented node compromise attack is addressed. When the system achieves its equilibrium, as explained in Theorem 1 in Sec. 3, each vehicle transmits $\frac{E_2}{n_0}$ packets to achieve the optimal hybrid utility (credit) rewarding for both packet forwarding and security consideration. The reason is that in Eqn. (2a), the components $\frac{E_2}{n}$ and $\left(1 - \frac{E_2}{n_0}\right)n$ precisely reflect negative effect on vehicle 1 brought by both the competition for forwarding packets between vehicles and the targeting-oriented node compromise attack (Eqn. (2b) is constructed the same way). The fairness is simultaneously realized by the fact that each vehicle transmits equal number of packets ($\frac{E_2}{n_0}$) for credit earning. Additionally in Sec. 3, if the number of packets carried by one intermediate vehicle exceeds $\frac{E_2}{n_0}$, it will automatically share the opportunity of transmitting packets to other vehicles since more transmitted packets cannot bring it more credits.

B. Free Riding Attack

The free riding attack refers to the malicious behavior of two selfish intermediate vehicles which are intended to exchange messages without paying credits [10]. If the colluding nodes are adjacent to each other, it is invaluably to launch this attack, since they can directly exchange messages without the aid of others. However, the case is absolutely different when at least one intermediate vehicle located in between them. It is assumed that $\mathcal{N}_i$ wants to transmit the message $m'$ to $\mathcal{N}_{i+2}$ with the help of $\mathcal{N}_{i+1}$, by piggybacking it with the forwarded bundle packet $P_b, B L, E L_1, \ldots, E L_i$. However, the packet transmitting commitment $\text{Signs} = H_1(S)^{S_1}, H_0(P || \text{Info}_{OS})$ generated by the source vehicle perfectly protect the integrity of $P_b || \text{Info}_{OS}$, therefore, the free riding message $m'$ cannot pass the verification and $\mathcal{N}_{i+2}$ will detect this kind of attack before transmitting $m'$ to $\mathcal{N}_{i+2}$.

C. Privacy-Preserving Aggregated Transmission Evidence Generation

We formally prove the privacy preservation of our aggregated transmission evidence generation. Firstly, it is straightforwardly observed that the distributed vehicular clouds cannot derive the individual velocity $V_{ij, S} \rightarrow L_1, T_{S}$ collected by RSU $l(l \neq k)$, since it is blinded by the random number $r_{i,l}$ selected by RSU $l$ which can still not be known by each vehicular cloud $k$ even though $r_{i,k, T} = \sum_{i=1}^{n_l} r_{i,l}$ is publicized. Then, we give the formal proof that the average velocity $V_{l_j, S} \rightarrow L_1, T_{S}$ (i.e. apparently also the aggregated cluster velocity $V_{l, T}$) which is used to generate the aggregated transmission evidence can only be recovered by the transportation manager TM.

Theorem 2: Let $\mathcal{A}$ be a malicious adversary defeating our proposed privacy preserving aggregated transmission evidence generation (ATEG) with a non-negligible advantage defined as $Adv_{CCA_{ATEG}}^{CCA_{ATEG}^{\mathcal{A}(l, n(k))}}(k)$, where $n(k)$ refers to the total number of queries made to the oracles and $k$ is the security parameter. There exists a simulator $\mathcal{B}$ who can use $\mathcal{A}$ to invert the one-way trapdoor function with the probability:

$$\epsilon \geq Adv_{CCA_{ATEG}}^{CCA_{ATEG}^{\mathcal{A}(l, n(k))}}(k) - \frac{n(k)}{2^{k-1}}.$$ (23)

Proof: The proof is by contradiction. Let $\mathcal{A}$ be an adversary that can successfully defeat the proposed construction, then there exists an polynomially-efficient algorithm $\mathcal{B}$ that can invert the one-way trapdoor function by the interaction with the adversary $\mathcal{A}$. In the initialization phase, the system performs $(f, f^{-1}, \mathcal{R}) \leftarrow \mathcal{G}(1^k), r_l \leftarrow \mathcal{G}(d(1^k)), y = f(r_l), r_{i,k, T} \in_R \mathcal{G}$ and the simulator $\mathcal{B}$ tries to solve $f^{-1}(y)$. There are three oracles, namely $\mathcal{O}_{\text{H}_1}$, $\mathcal{O}_{\text{H}_2}$ and $\mathcal{O}_{\text{Dec}}$. $\mathcal{B}$ can perform the simulations by answering the queries from the adversary as follows.

$\mathcal{O}_{\text{H}_1}$ Query. If a query $r_l \parallel r_{i,k, T}$ to $\mathcal{O}_{\text{H}_1}$ satisfies $f(r_l) = y$, then $B$ outputs $r_l$ and halts; else it returns a random element $Str_3 \in \mathcal{R}$ as the response to the adversary and remains the triple ($r_l, r_{i,k, T}, Str_3$) in the $H_1$-list.

$\mathcal{O}_{\text{H}_2}$ Query. To answer the query $C_{l,k, T} \parallel C_{k, ram}$, the simulator $\mathcal{B}$ firstly checks whether $C_{k, ram}$ is located in the $H_2$-list. If it does exist, $\mathcal{B}$ gives back a random number $Str_5 \in \mathcal{R}$ as the response to the adversary and remains the triple ($C_{l,k, T}, C_{k, ram}, Str_5$) in the $H_3$-list. Otherwise, it returns invalid.
\textbf{\(O_{\text{Dec}}\) Query.} To answer the query \(s \parallel d \parallel h\) to \(O_{\text{Dec}}\), the simulator \(\mathcal{B}\) firstly checks if there exists a triple \((d, C_{k, ram}, h)\) in the \(H_2\)-list satisfying the condition that \(C_{k, ram}\) has already appeared in the \(H_2\)-list. If it does, the simulator \(\mathcal{B}\) firstly looks up in the \(H_4\)-list to find the corresponding \(r_i, r_{i,k,T}\) w.r.t. \(C_{k, ram}\) and computes \(V_{i,T} = (d - r_{i,k,T})r_i^{-1}\). Finally, it checks whether \(s = f(r_i)\) holds and returns \(V_{i,T}\) as the response. Otherwise it returns invalid.

Then, the adversary \(\mathcal{A}\) submits two messages \(m_0, m_1 \in \mathbb{R}\), and the simulator \(\mathcal{B}\) randomly selects \(\beta \in [0,1]\) and returns the encryption of \(m_\beta\) as the challenge ciphertext \(c^*\). After receiving \(c^*\), \(\mathcal{A}\) can continue to make queries to the oracles \(O_{H_6}, O_{H_5}\) and \(O_{\text{Dec}}\) with the restriction that \(c^*\) cannot be queried to the decryption oracle \(O_{\text{Dec}}\) in the adaptive query phase.

To explain the interactions perfectly simulating the real environment of the adversary \(\mathcal{A}\) running with its oracles, we focus on the following events. Let \(S\) denote the event that for some ciphertext \(s \parallel d \parallel h\), \(\mathcal{A}\) made some query \(d \parallel h \parallel C_{k, ram}\) to the oracle \(O_{H_6}\) where \(C_{k, ram}\) has existed in the \(H_2\)-list and the corresponding \(r_i\) w.r.t. \(C_{k, ram}\) satisfying \(f(r_i) = \alpha\). Then, we further let \(R\) be the event that \(\mathcal{A}\) made some query \(s \parallel d \parallel h\) to the decryption oracle \(O_{H_6}\) where \(C_{k, ram}\) has existed in the \(H_2\)-list and \(C_{k, ram} = H_4(f^{-1}(s) \parallel r_{i,k,T})\) hold without making any query \(f^{-1}(s) \parallel r_{i,k,T}\) to the \(H_4\)-oracle or \((d \parallel C_{k, ram})\) to the \(H_2\)-oracle where \(C_{k, ram}\) appears in the \(H_2\)-list. Let \(n(k)\) be the total number of oracle queries made by the adversary \(\mathcal{A}\). Then, we can conclude that

\[
Pr[\mathcal{A}^{\text{Suc}}] = Pr[\mathcal{A}^{\text{Suc}}|R]Pr[R] + Pr[\mathcal{A}^{\text{Suc}}|\bar{R} \land S]Pr[\bar{R} \land S] + Pr[\mathcal{A}^{\text{Suc}}|\bar{R} \land \bar{S}]Pr[\bar{R} \land \bar{S}]
\leq n(k)2^{-k} + Pr[S] + \frac{1}{2}, \quad (24)
\]

since \(Pr[R] \leq \frac{n(k)}{2} \) and \(Pr[\mathcal{A}^{\text{Suc}}|\bar{R} \land \bar{S}] = \frac{1}{2}\) can be straightforwardly derived. Finally, it is observed that the probability of simulator \(\mathcal{B}\) to fail in behaving like the adversary \(\mathcal{A}\) in inverting the one-way trapdoor function \(f()\) can be bounded by \(Pr[R]\). Therefore,

\[
\epsilon \geq Ad_{CC}^{AT\text{EG}}\mathcal{A}^{\text{AT\text{EG}}}(\alpha, n(k))(k) - \frac{n(k)}{2^{k-1}}, \quad (25)
\]

which is also non-negligible and Theorem 2 holds.

\textbf{D. Layer-Removing/Adding Attack}

The layer-removing attack can be launched by a group of selfish vehicles to remove all the forwarding layers in between them to maximize their rewarded credits [10]. As the packet forwarding phase explained in the previous section, each intermediate vehicle possesses two valid packet transmitting witnesses which can effectively prove its participation in the cooperation of packet forwarding, namely \(\text{Sig}_{N_{t+1}} \leftarrow H_1(\{N_{i+1}\})^yH_3(P_k || BL || T_{S_i} || N_i || L_i || \text{Index}_i)\) signed by \(N_{t+1}\) and \(\sigma_{i-1,1} = \sigma_{i-1,1}X_{i-1}Y_{i-1}H_2(N_{i-1})^{2}H_1(\{N_{i-1}\})^{y_1}H_3(\{N_{i-1}\})^{y_2}P_k || BL || N_{i-1} || N_i || L_{i-1} || T_{S_{i-1}} || \text{Index}_{i}|| H_4(f_{i-1})\) composed in \(\text{Sig}_{N_i}^{\text{agg}}\) signed by \(N_{i-1}\). If two selfish vehicles launch the layer-removing attack, those removed intermediate vehicles can submit the witnesses to prove their contribution and the layer-removing attack can be well prevented. As a special kind of layer removing attack, the source vehicle \(S\) would collude with the last intermediate vehicle \(N_{\omega}\) to disenable the intermediate vehicles to be rewarded. However in our proposed TCBI, this attack is still hard to launch since the source \(S\) does not know the last intermediate vehicle \(N_{\omega}\); even though \(S\) knows \(N_{\omega}\) and generates the forged transmitting commitment \(\text{Sig}_{S,N_{\omega}} = H_1(S)^{y_1}H_3(P_k || BL || T_{S_i} || N_{\omega})\) for \(N_{\omega}\), it still cannot deny its signing on \(\text{Sig}_{S,N_i} = H_1(S)^{y_1}H_3(P_k || BL || T_{S_i} || N_i)\). Consequently, this collusion attack can also be detected.

Especially in this paper, we consider the layer-adding attack sponsored by the collusion of malicious vehicles. The purpose of colluding vehicles is to detract the packet forwarding path from the source to the destination for increased credits. Without loss of generality, \(N_i\) and \(N_{i+1}\) want to insert an additional endorsed layer \(N_{i+1}\) between them. Since the colluders have no knowledge of the velocities of the vehicle clusters moving from \(L_i\) to \(L_{i,i+1}\) and from \(L_{i+1}\) to \(L_{i+1}\) respectively, it is impossible for them to embed the correct time stamp \(T_{S_{i+1}}\) in the added endorsed layer \(E_{L_{i,i+1}}\) except a random guess. Therefore, if an incorrect time stamp \(T_{S_{i+1}}\) is used to compute the time period \(P_{E_{R_{i+1}}}\) for generating the aggregated transmitting commitment \(\text{Sig}_{S_{i+1}}^{\text{agg}}\), it cannot pass the verification performed by \(AC\) with the aggregated transmission evidence reported by \(TM\). Specifically, it is observed that the adversary can successfully launch the layer-adding attack by either breaking the underlying identity-based sequential aggregate signature or defeating our proposed privacy-preserving aggregated transmission evidence generation (ATEG) algorithm in the TCBI construction. Therefore, we can formally arrive at the following theorem of the resilience to layer-adding attacks for our proposed TCBI, which can be straightforwardly derived from Theorem 2 and the exploited identity-based sequential aggregate signature [13]. The proofs are detailed in the supplemental materials.

\textbf{Theorem 3:} Let \(\mathcal{A}'\) be a malicious adversary successfully launching layer-adding attacks in our proposed TCBI with a non-negligible advantage defined as \(Ad_{\mathcal{A}'}^{\text{UF-IBAS}}(k)\), where \(k\) is the security parameter. There exists a Simulator \(\mathcal{B}'\) who can use \(\mathcal{A}'\) to either invert the one-way trapdoor function with the non-negligible probability when the underlying identity-based sequential aggregate signature is secure namely \(Ad_{\mathcal{A}'}^{\text{UF-IBAS}}(\alpha, n(k))(k)\) is negligible:

\[
\epsilon_{\text{OWTF}} \geq Ad_{\mathcal{A}'}^{\text{UF-IBAS}}(k) - Ad_{\mathcal{A}'}(\alpha, n(k))(k) - \frac{n(k)}{2^{k-1}}, \quad (26)
\]

or solve the IBSAS-CDH problem with the non-negligible probability when our proposed privacy-preserving aggregated transmission evidence generation (ATEG) is secure namely.
AdvCCA\textsuperscript{ATEG}_{A'(t,n(k))}(k) is negligible:
\[ \epsilon_{BSAS-CDH} \geq \frac{Adv Lay ADD_{A'}^TCBI(k) - AdvCCA\textsuperscript{ATEG}_{A'(t,n(k))}(k)}{e(n'(k)(q_t + 1) + q_K)} - \frac{q^2_h/l_{\text{min}}(\text{Gen})}{e(n_{\max}(q_t + 1) + q_K)} \] (27)
where (k) refers to the most query times made to the oracles \(O_{\text{Dec}}\) and \(O_{\text{H1}}, O_{\text{H2}}\) of the privacy preserving aggregated transmission evidence generation (ATEG) algorithm; \(l_{\text{min}}(G)\) refers to the minimum bit-length of the prime order \(p\) of a bilinear group output by Gen, \(q_h, q_K, q_\ell\) denote the most query times to the hash oracles, the key-derivation oracle and the signing oracle with \(n'(k)\) as the maximal length of the output lists in the exploited identity-based sequential aggregate signature [13].

VI. PERFORMANCE EVALUATION

In this section, we evaluate the performance of our proposed TCBI in terms of computational and communication overhead, delivery ratio and average delay by extensive simulations using a custom simulator built in Java.

A. Efficiency Comparisons

Our proposed TCBI exploits the average velocity of the vehicular cluster \(V_{L_5\rightarrow L_1, T_{S_5}}\) derived from the aggregated vehicular velocity \(V_{I,T}\) to generate the aggregated transmission evidence. It not only satisfies the security and privacy requirements of data aggregation as explained in the previous section, but also possesses the following unique and significant characteristics. (1) Any one-way trapdoor function can be exploited to realize the privacy preserving aggregated transmission evidence generation. (2) The one-way trapdoor function computation is required to be performed only once for aggregating multiple individual vehicle velocity in each time period.

We study the performance by exploiting PBC [27] and MIRACLE [29] libraries running on Linux platform with 2.93GHz processor. The experimental results show a single exponentiation and multiplicative operation in \(\mathbb{Z}_{N^2}(|N| = 1024)\) almost respectively cost 12.6 ms and 10.4 ms. The same operations in the multiplicative group of the skew field \(\mathbb{R}\) with the prime order \(p\) almost respectively cost 6.2 ms and 5.1 ms. In our simulation, ElGamal encryption is exploited to implement the one-way trapdoor function in our proposed TCBI. Since compared to SMART protocol [9], our proposed TCBI embraces an additional algorithm (function) of Aggregated Transmission Evidence Generation, where a new efficient privacy-preserving outsourced data aggregation is devised for the vehicular cloud to compute the aggregated transmission evidences for intermediate vehicles cooperating to forward packets, we integrated the most adopted Paillier’s additive homomorphic cryptosystem [33] into [9] to allow it to hold the same functionalities as our proposed TCBI. Then, we compare the corresponding computational and communication cost to demonstrate the efficiency advantage brought about by our newly-designed Aggregated Transmission Evidence Generation algorithm, and hence the proposed incentive mechanism TCBI over the SMART protocol [9]. The evaluation results are the average of repeating the same experiment 1000 times. Fig. 3 shows as the number of vehicles in each cluster increases, for both the RSUs collecting/generating the raw encrypted vehicle velocity data and the disengaged RSUs serving the function as the distributed cloud in VANETs, the computational cost of the SMART protocol [9] is significantly heavier than our proposed TCBI. The critical reason is that in our proposed TCBI, it is required to perform only once the underlying one-way trapdoor function (i.e. the ElGamal encryption on the randomly selected blinding factor \(r_{1}\)) for aggregating \(n_\ell\) vehicular velocity data. On the contrary, the modified SMART protocol adopting Pallier’s Cryptosystem [33] as a cornerstone requires one Pallier’s encryption on each piece of velocity data, which loads a dramatically increased computational cost on the RSUs which would become a bottleneck when large number of vehicles are passing by especially along the main streets. Fig. 4 illustrates the communication cost of our proposed TCBI on the side of the RSUs sending the raw encrypted velocity data is almost half as the modified SMART protocol [9]. This significant enhancement mainly owes to the fact that each ciphertext of Pallier’s cryptosystem [33] is in \(\mathbb{Z}_{N^2}(|N| = 1024)\); while in our proposed TCBI, the session key is required to be negotiated only once in the one-way trapdoor function \(f(\cdot)\), implemented by ElGamal encryption in \(\mathbb{Z}_{p}(|p| = 512)\). Therefore, the total size of the ciphertexts w.r.t. the individual vehicular velocities would be dramatically saved.

B. Simulation Settings

In our simulation, total n DTN vehicular nodes with a transmission radius of 300 meters are uniformly deployed in an area of 6000m \(\times\) 10000m and the shortest path map based
movement routing is selected since the message is forwarded by the vehicles moving along the streets. In this scenario, each vehicle randomly selects a destination and moves there for a 2 min. pause, then it repeats the above until the simulation is done. Let the selfish ratio \( \beta = \frac{\text{Num of Selfish Vehicles}}{\text{Total Num of Vehicles}} \). The larger the selfish ratio is, the more vehicles are unwilling to forward packets. \( r_0 \) is defined as the probability of successfully sponsoring a node compromise attack and \( r_g \) refers to the average packet generation rate of the underlying vehicular DTNs. Other useful parameter settings in the simulations are illustrated in Table II. For each case, we perform the experiment for the associated time period varying from 1 to 10 hours with the increment of 1 hour. For each time period, the average delivery ratio and average delay are reported after ten times of simulation.

C. Simulation Results

In Fig. 5, we compare the delivery ratio under different selfish ratio \( \beta = 0, 30\%, 90\% \) and successful node compromise probability \( r_0 = 0.3 - 0.5, 0.7 - 0.9 \) when the average packet generation ratio \( r_g \) is fixed to 25-35. It shows that the delivery ratio decreases as the selfish ratio and the successful node compromise probability respectively increases. The reason is that when the selfish ratio is larger, it is more difficult for each intermediate vehicle to find a successor willing to relay the packets. Additionally when \( r_0 \) is larger, the probability of vehicles located in multiple routings from the source to the destination to be compromised will be significantly increased. For each transmitted message, there would be more packets intercepted, modified or dropped and in our proposed \( (t,n) \) threshold incentive mechanism TCBI, the probability of successfully recovering the original message, namely the actual delivery ratio at the destination would decrease.

In Fig. 6, the delivery ratio is compared under various conditions of \( \beta = 0, 30\%, 90\% \) and \( r_g = 25 - 30, 50 - 100 \), when the \( r_0 \) is fixed to 0.5. It shows that the delivery ratio decrease as the selfish ratio and the average packet generation ratio respectively increases. The selfish ratio contributes to the delivery ratio the same as the scenario in Fig. 5. A larger average packet generation ratio means there are more packets generated in each time period of fixed length. Since the resources including the storage capacity of OBU equipped on vehicles are stringently constrained, it is definite that more packets will be dropped for the reason that they cannot find another intermediate vehicle to forward the packet in \( TTL \).

Fig. 7 illustrates the delivery ratio varies with the number of forwarding packet shares (threshold) from 1 to 50 under different vehicle compromise probabilities. It shows when the compromise probability \( r_0 = 0.3, 0.5, 0.8 \), the delivery ratio respectively increases at first until the number of forwarding packet shares reaches approximately the optimized thresholds \( t = 10, 20, 35 \); and then smoothly decreases as the packet share number continues to increase. The reason is that when the number of packet shares is small, its increase benefits to the message recovery in our proposed \( (t,n) \) threshold incentive mechanism TCBI. However, when it exceeds some threshold, the total number of packets will be out of the tolerance of the constrained storage capacity of OBUs and a considerable part of them would be dropped. On the other hand, it is observed that as the compromise probability increases (i.e. the number of secure multi-paths available for packet transmission decreases), it is required to increase the threshold \( t \) for successful message delivery since more packet shares would be obtained, interrupted and modified by the adversary. More significantly, the message is firstly encrypted and encoded into shares transmitted through multiple routings. Therefore, the adversary cannot derive the original message even they have.
compromised threshold number of packet shares w.r.t. one specific message without the decryption key. Therefore, the threshold $t$ of our proposed TCBI can be flexibly selected by jointly considering different network states such as the security, reliability and the performance requirement.

Fig. 8(a) shows the average delay decreases as the number of packet shares increases and it also decreases as vehicle compromise probability $r_0$ increases. Fig. 8(b) illustrates the average delay reported in the different groups of simulations with the selfish ratio $\beta$ varies from 0, 30% to 90% in each group. From groups 1 and 2 with $r_0 = 0.3 - 0.5, 0.7 - 0.9, r_\beta = 25 - 35$, we conclude the average delay increases as the successful node compromise probability increases. From groups 3 and 4 with $r_\beta = 50 - 100, 25 - 30, r_0 = 0.5$, it is observed that the average delay decreases as average packet generation rate increases.

Then, we compare the delivery ratio and the average delay among the existing work SMART [9], Pi [10], the packet forwarding in vehicular DTN without security protection and our proposed TCBI under the same suit of simulation parameters. Fig. 8(c) shows that the delivery ratio of our proposed TCBI is significantly higher than the SMART scheme [9], Pi scheme [10] and the one without any security guarantees. The reason is that our proposed threshold credit-based incentive mechanism TCBI and the corresponding secure and privacy-preserving packet forwarding protocol can effectively resist packet injection, interruption, modification and even target-oriented vehicle compromise attack, which dramatically benefits to successful delivery. Fig. 9(a) demonstrates that the average delay of our proposed TCBI is slightly higher than the existing schemes [9], [10]. The reason is that to efficiently resist target-oriented node compromise attack, the $(t, n)$ secret sharing scheme is exploited and redundant packets are transmitted to enhance delivery reliability. On the other hand, the equilibrium $n_{eq}^m = \frac{\tau}{2r_0}$ in Theorem 1 restricts the number of data packets transmitted by each intermediate vehicle, which would increase the average delay in our proposed TCBI. It can be considered as a tradeoff between the security and efficiency.

Finally, we evaluate privacy preserving vehicle clustering overhead and the packet routing overhead in our proposed TCBI. By implementing $f_s, f_j$ with ElGamal encryption on $\mathbb{Z}_p (|p| = 512\text{bit})$, Fig. 9(b) illustrates the computational cost of secure vehicle clustering. As the number of clusters $K$ and vehicles $N$ increases, both of the computational cost of vehicles and cluster heads increases accordingly, since more privacy-preserving distance computations and comparisons are required for secure clustering. By implementing each component of the base layer as 4-byte long, with the exception that the signatures $\text{Sig}_S, \text{Sig}_{N_1}, S, \text{Sig}_N$ and certificates $\text{Cert}_S, \text{Cert}_{N_1}$ are of 20-byte long, Fig. 9(c) illustrates the communication overhead for packet routing decreases as the routing threshold $t' \leq \frac{\tau}{2r_0} < t$ and the vehicle number respectively increases, since $N_i$ is likely to successfully find a successor by checking less candidates $N_{i+1,k} (k = 1, 2, \cdots)$, namely, less packet transmitting responses $\text{Sig}_{N_{i+1}}$ are required to generate for selecting a transmitter in the next hop.

VII. RELATED WORK

The high moving velocity of vehicles makes the underlying DTNs lacking of continual routings and its
unique characteristic of selfishness leaves a series of existing incentive mechanisms cannot be directly applied to vehicular DTNs. Recently, the following research work on incentive mechanism based packet forwarding are reported [9], [10], [16]–[26], [28], [34]–[37], closely relating to our proposed TCBI.

Shen et al. firstly studied the negative effect brought about by the selfish nodes in DTNs [24]. They showed the existing DTN nodes significantly degrades the delivered traffic by extensive simulations. To solve the problem, a practical incentive mechanism pairwise tit-for-tat (TFT) was proposed. Based on it, an incentive aware routing protocol was devised to maximize the utility of selfish DTN nodes. However, no security issues were addressed in their work. Zhu et al. proposed a secure multi-layer credit-based incentive scheme (SMART) [9] to stimulate bundle forwarding cooperation among DTN nodes. It can resist various kinds of attacks such as layer injection attack and nodular timeout attack and several efficiency optimization techniques were utilized to improve the overall performance. Different from SMART, Lu et al. proposed a secure and practical incentive protocol Pi in DTNs focusing on the fairness issue in DTNs. They attached some incentive on the bundle and designed a hybrid charging and rewarding strategy [10], not only attractive but fair to all DTN nodes. Recently, Zhu et al. proposed a probabilistic misbehavior detection scheme towards efficient trust establishment in DTNs [36] and Lin et al. designed a mechanism to address the sybil attack in vehicular peer-to-peer networks [37]. However, as to the security aspect, the existing work [9], [10], [36], [37] only considered the outsider attacks, leaving the more sophisticated target-oriented node compromise attack which could be easily launched in vehicular DTNs untouched. Moreover, the fair incentive scheme for single-copy algorithms is no further appropriate for the above-mentioned threat model, since once the single message is compromised, the original message can never be recovered. Finally, how to resist the colluding of different DTN nodes to sponsor layer-adding attack is still a challenging issue proposed in [10].

To realize secure and privacy-preserving data aggregation, significant advances have taken place in the field of fully homomorphic encryption serving as a steppingstone [30]–[33]. However, some intrinsically unsolvable problems significantly impedes its wide application in practice. Most existing work [31]–[33] is mainly constructed based on the polynomially-bounded hard problems in lattice and the plaintext has to be encrypted bit-by-bit, the computational complexity of which makes it invaluable for the scenarios where large volumes of data are frequently collected and computed such as the vehicular ad hoc networks and the smart grid communications. Therefore, how to design a secure and privacy preserving data aggregation with dramatically enhanced efficiency especially on the ends of resource-constrained mobile devices is a challenging open problem requiring practical solutions.

Different from the existing works, in our paper, a threshold incentive scheme (TCBI) is proposed to efficiently resist the newly-identified target-oriented node compromise attack and realize the fairness in both sharing the equal opportunities of transmitting packets among vehicles and devising effective charging and rewarding policies. Additionally, the advantages of CV-DTNs are taken into consideration when generating transmission evidence to resist the collusion for launching layer-adding attacks, where a great deal of privacy-preserving data aggregation tasks are delegated to the vehicular cloud composed of disengaged vehicles and the underlying one-way trapdoor function is required to perform only once at the vehicle’s side to aggregate multiple pieces of individual velocity data.

VIII. Conclusion

In this paper, a novel threshold credit-based incentive mechanism TCBI is proposed based on the modified model of population dynamics to prevent the node compromise attacks, stimulate the cooperation for packet forwarding, realize the fairness and maximize interests among vehicles. Based on it, our proposed TCBI-based secure and privacy-preserving packet forwarding scheme effectively solves the open problem of resisting layer-adding attacks. Both the individual vehicle velocity privacy and the cluster moving velocity privacy are well protected from the semi-trusted vehicular cloud, the malicious vehicles and even their collusions. Finally, the security analysis and the extensive simulations demonstrate the effectiveness and practicability of our proposed TCBI.

References


Jun Zhou is currently pursuing the Ph.D. degree in computer science with the Trusted Digital Technology Laboratory, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China. He has been with East China Normal University since 2014. His research interests mainly include secure e-healthcare systems, and privacy preserving outsourcing computation in cryptography and information security.

Xiaolei Dong is a Distinguished Professor in East China Normal University. After her graduation with a doctorate degree from Harbin Institute of Technology in 2001, she pursued her post-doctoral study in SJTU from September 2001 to July 2003. She joined the Department of Computer Science and Engineering, SJTU, in 2003. In 2014, she joined East China Normal University, where she is currently a Distinguished Professor. Her primary research interests include number theory, cryptography, and trusted computing. Her Number Theory and Modern Cryptographic Algorithms project received the first prize of the China University Science and Technology Award in 2002. Her New Theory of Cryptography and Some Basic Problems project received the second prize of the Shanghai Science and Technology Award in 2007. Her Formal Security Theory of Complex Cryptographic System and Applications project received the second prize of the Ministry of Education National Science Progress Award in 2009. Her research projects supported by the National Basic Research Program of China (973 Program), and the special funds on information security of the National Development and Reform Commission, and the National Natural Science Foundation of China.

Zhenfu Cao (SM’10) received the B.Sc. degree in computer science and technology and the Ph.D. degree in mathematics from the Harbin Institute of Technology, Harbin, China, in 1983 and 1991, respectively. He was exceptionally promoted to Associate Professor in 1987, became a Professor in 1991, and is currently a Distinguished Professor with East China Normal University, China. Since 1981, over 400 academic papers have been published in journals or conferences. His research interests mainly include number theory, cryptography, and information security. He serves as a member of the Expert Panel of the National Nature Science Fund of China. He has received a number of awards, including the Youth Research Fund Award of the Chinese Academy of Science in 1986, the Ying-Tung Fok Young Teacher Award in 1989, the National Outstanding Youth Fund of China in 2002, and the Special Allowance by the State Council in 2005. He was a coreipient of the 2007 IEEE International Conference on Communications-Computer and Communications Security Symposium Best Paper Award in 2007. He is the Leader of the Asia 3 Foresight Program (61161140320), and the key project (61033014) of the National Natural Science Foundation of China.

Athanassios V. Vasilakos is currently a Visiting Professor with the National Technical University of Athens, Greece. He served as an Editor of many technical journals, such as the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, the IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B, the IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, the ACM Transactions on Autonomous and Adaptive Systems, and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS Special Issues in 2009 and 2011. He is the Chairman of the Council of Computing of the European Alliances for Innovation.