A Secure Reed–Solomon Code Incentive Scheme for Commercial Ad Dissemination Over VANETs

Fu-Kuo Tseng, Yung-Hsiang Liu, Jing-Shyang Hwu, and Rong-Jaye Chen

***Abstract*—A recent surge of research on *vehicular ad hoc networks* (VANETs) has given us new opportunities and challenges. Aside from safety-related applications, commercial applications also find their way to fully utilize these networks. One of the promising applications is the dissemination of commercial advertisements over VANETs. However, there are uncooperative vehicles that may disrupt the spreading of these advertisements. To encourage cooperation, we want to address proper incentives and security measurements. In this paper, we use Reed–Solomon codes (RS-codes) to construct our incentive scheme and enhance its security by introducing one discrete logarithm representation problem. Our construction yields a secure and practical commercial advertisement dissemination scheme over VANETs.**

***Index Terms*—Cooperation enforcement, incentive schemes, packet forwarding, Reed–Solomon codes (RS-codes), vehicular ad hoc networks (VANETs), vehicular applications.**

I. Introduction

RECENT YEARS have seen increased attention given to *vehicular ad hoc networks* (VANETs). These networks contain a large number of vehicles and *roadside units* (RSUs) [1], [2]. Each vehicle has an *onboard unit* (OBU) to communicate with other OBUs or RSUs. In other words, OBUs and RSUs can communicate and exchange information. This technology is part of telematics that utilizes telecommunication and informatics to achieve the following three major goals in the vehicular environment: 1) safety; 2) convenience; and 3) entertainment. Government, industry, and academia have allocated many resources into establishing the VANET standards to meet the aforementioned goals. Many VANET testbeds are designed, and field trials are conducted to turn the theory into practice. By carrying out these new applications over VANETs, we will achieve safer navigation, more convenience, and more fun on the road.

Although safety-related applications [3]–[8] are the prime motivation behind VANETs, these networks also provide good platforms for large-scale highly mobile applications. Driven by potential profits, commercial-related development has been geared to fully utilizing these networks [9]–[15]. One of the promising applications is the dissemination of commercial advertisements [12], [13]. A vehicle could receive advertisements from its neighboring vehicles and redistribute them along its path. The method is simple and effective. However, in reality, the existence of uncooperative vehicles may disrupt this application. Furthermore, some uninterested drivers may ignore whatever information forwarded to them and act passively, whereas other clever drivers try to maximize their advantages but dodge responsibility. In addition, malicious drivers can invoke attacks to paralyze some specific vehicles or the entire network. Even among cooperative vehicles, some drivers may doubt whether they need to relay advertisements for the benefits of advertising companies.

There are two main research areas that are related to the data dissemination over wireless networks or VANETs [16]. One area is routing through a dedicated routing path, and the other area is flooding and relaying to the neighboring vehicles. For the former area, there are source and destination nodes involved in transmitting their data packets. The nodes situated in between serve as routing points to forward the packet. In these protocols, a routing path should be decided before the data are transmitted. The intermediate nodes agree on forwarding the packets. They may either report to the infrastructure or carry the necessary information to be rewarded later with a certain amount of credits. These credits are usually provided by both source and destination vehicles, because both of them benefit from the transmission. There have been several reliable solutions on this research topic, as shown in [17] and [18].

Our aim falls into the latter case—flooding and relaying to the vehicles within some specific areas. There exists one source node to spread advertisements. However, the recipients are those who drive within one particular area rather than toward one specific destination or vehicle. This case is related to geographic broadcast or Geocast. Therefore, the routing path may not be decided before relaying the packet, and only the location information of the neighboring nodes and the source node is needed. The goal of this paper is to utilize the mobile ad hoc networks to spread the information to any nodes within certain parts of the networks.

Several existing protocols [17]–[25] have been proposed to stimulate cooperation among network nodes by designing routing protocols or relaying schemes. The proposed solutions are mainly divided into the following two categories: 1) reputation-based systems and 2) incentive-based systems. In reputation-based systems, each network node watches and checks the transmission of its neighbors. It also computes and publishes reputation scores for a set of its neighboring nodes. The network

Manuscript received January 30, 2011; revised June 22, 2011 and October 7, 2011; accepted October 7, 2011. Date of publication October 18, 2011; date of current version December 9, 2011. This work was supported in part by the National Science Council of Taiwan under Contract NSC98-2221-E-009-079-MY3 and by the Industrial Technology Research Institute of Taiwan under Grant A3522U4100. The review of this paper was coordinated by Dr. S. Zhong.

F.-K. Tseng, Y.-H. Liu, and R.-J. Chen are with the Department of Computer Science, National Chiao Tung University, Hsinchu 30010, Taiwan (e-mail: fktseng@cs.nctu.edu.tw; liuyh@cs.nctu.edu.tw; rjchen@cs.nctu.edu.tw).

J.-S. Hwu is with the ICT Design and Validation for Vehicles Department, Telematics and Vehicular Control System Division, Information and Communications Research Laboratory, Industrial Technology Research Institute, Hsinchu 31040, Taiwan (e-mail: jshwu@itri.org.tw).

Digital Object Identifier 10.1109/TVT.2011.2172471

administrator can identify the uncooperative nodes and exclude them from the networks. In other words, this scheme treats as obligation the forwarding of the packets of network nodes. On the contrary, in the incentive-based scheme, the forwarding job is treated as a service, which is also called the metered service or pay-per-use service. The incentives can range from the virtual cash to the voucher to exchange for commodities. In our design, the goal is to launch a commercial campaign over a particular area during specific time interval, and the participating vehicles can be rewarded with corresponding compensation.

However, reputation-based systems [24], [25] depend on continuously monitoring the neighboring nodes, which consumes a large amount of computation resources. In addition, it is also possible that forwarded packets fail to reach the destination and result in biased rating for the intermediate nodes involved. Furthermore, the rating mechanism is based on the probed data of the neighboring nodes, which are usually inaccurate, and is vulnerable to colluders. A set of nodes can collude and lift their reputations. It is also difficult to distinguish between the node's refusal to cooperate and the inability to carry out the task, because there are times when vehicles are short of power or lack communication links.

Thus, incentive-based systems [17]–[23] provide a better design for cooperation. When packets are forwarded, the owner or even the receiver should provide corresponding compensation to the intermediate nodes. This condition envisions future charging mechanism over mobile ad hoc networks. The common limit of these designs is the need for a growing size of relayer records and for the interaction among the intermediate nodes. Therefore, our goals and also our contributions are to design a secure and practical incentive scheme to meet the following four requirements.

1) *All* cooperative vehicles are rewarded with incentives, whereas uncooperative vehicles cannot gain *any* advantage.
2) Cooperative vehicles can be identified within one single operation over the relayer record.
3) The size of relayer records is constant rather than proportional to the number of cooperative vehicles.
4) The number of communication between vehicles is minimized to one single broadcast, and no interaction between vehicles is needed.

We were inspired by the traitor-tracing schemes in [26] and [27], where the traitors that contribute to the pirate decoder are caught through the use of Reed–Solomon codes (RS-codes). We tailored these schemes by removing unnecessary parts and designed corresponding protocols to yield a secure and practical incentive scheme to disseminate commercial advertisements over VANETs. We also made comparison with previously proposed schemes and conclude that our scheme uniquely fulfills the aforementioned four requirements.

The rest of this paper is structured as follows. Representative related works are presented in Section II, whereas system models are detailed in Section III. Next, Section IV elaborates on our designs, including the notation used and the operations performed by each of the system principals. Then, Section V presents security analysis and performance evaluation, including further consideration of our design for different applications. Section VI concludes by reiterating our contribution and addressing possible future work.

II. Related Work

To encourage cooperation, many advertising companies are more than willing to provide incentives. Several incentive-based relaying schemes have been proposed [17], [20], [21]. Most of these schemes leverage digital signature provided by *public key infrastructure* (PKI) for the integrity of the message. Drivers can be assured of the authenticity of the advertisement by verifying the appended signature of the *certificate authority* (CA).

These incentive schemes can roughly be divided into the following four categories:

1) signature counting;
2) receipt counting;
3) proportional rewarding;
4) weighted rewarding.

The signature-counting scheme is a straightforward approach that utilizes the so-called *credit claim*. As described in [20], a vehicle driver could append his/her credit claim to the advertisement and then distribute the advertisement. Any other vehicle could redistribute in the same way by appending its credit claim to the claims appended before. The authority-delegated RSUs would later gather over the network the advertisements and the credit claims appended. These records are analyzed and recognized to yield the list of the cooperative vehicles, which are given back credits later. Two main drawbacks of this kind of scheme are given as follows: 1) the growing communication overheads to transmit the advertisement and its corresponding credit claims and 2) the possibility of removing some credit claims along the path without being detected.

On the other hand, the receipt-counting scheme uses the *voucher* concept [21]. Anytime one vehicle broadcasts an advertisement, it asks for the vouchers from the vehicles that receive the advertisement. Vehicles try to collect as many vouchers as possible to be rewarded credits later by the authority-delegated RSUs. This scheme depends on the need for interactions between vehicles, which is often troublesome and hard to achieve because of the different speed and directions of the vehicles. To briefly sum up, the biggest problem for counting approaches is that they all suffer from overspending problems. The incentive provider cannot know in advance the total amount of rewards needed for each advertisement. They cannot control the spending on one specific commercial campaign. To counter the overspending problem, a fixed amount of rewards is predefined and then distributed according to the proportional contribution of each relayer. In these schemes, the source node agrees on the total amount of credits. When the packet reaches the destination, each participating nodes report their evidence of contribution to the coordinators. The total amount of the contribution can be assured, as is the fairness among relayers. However, it also brings new challenges. If the potential relayers try to maximize their own profits, they will finally keep the data and refuse to relay the packets, because they do not need to share the rewards with subsequent relayers.

Another approach for coping with the overspending problem is weighted rewarding schemes [17], which adjust the rewarding rules to encourage their cooperation. Although the latter two types of schemes appear to achieve high level of fairness, they have to deal with clever and cunning drivers that try to gain more advantages. In addition, they are more complicated than the former two types and may seriously affect the normal traffic. Therefore, we focus on designing an incentive scheme that is less complicated and achieves a satisfactory level of fairness. We also compare our incentive design with the typical schemes of signature and receipt counting [20], [21].

III. System Models

In this section, we present the overview of our system models, including network and communication models (see Section III-A), threat and trust models (see Section III-B), the goal model (see Section III-C), and the payment model (see Section III-D).

A. Network and Communication Models

We consider a general VANET that contains a large number of RSUs and vehicles equipped with OBUs. We also assume that each vehicle i has a unique nonzero identifier ID_i, which can be used to identify this vehicle. For brevity, we interchangeably use the terms ID_i, driver i, and OBU_i hereafter to identify vehicle i when no confusion is caused.

We assume that each vehicle can communicate with any other nearby vehicles or with roadside infrastructure to perform some useful applications such as safety-related functions or value-added telematics services. Considering the high-mobility nature of vehicles and their ad hoc communication characteristics, VANETs are regarded as the most promising mobile ad hoc networks.

We also assume that each registered vehicle keeps its own certificates: one certificate is issued by CA, and the other certificate is issued by a *vehicular authority* (VA), which is the specialized CA for vehicular networks. Usually, governmental authorities play the role of CAs, whereas governmental transportation departments are the VAs. VAs are in charge of the digital signature used for advertisement distribution and advertisement relayer tracing. There is a hierarchy of VAs that govern vehicles and RSUs within their jurisdiction. Vehicles can generate the content of packets or act as a packet-relayer for the incoming traffic. In our scheme, vehicles play the role of advertisement relayers. On the other hand, RSUs are usually treated as the extension of VAs and act as certificate management endpoints. RSUs also serve as access points and probe entries for the applications over VANETs. In our scheme, RSUs are responsible for injecting advertisements to VANETs and gather credit claims from the networks to VAs (see Fig. 1).

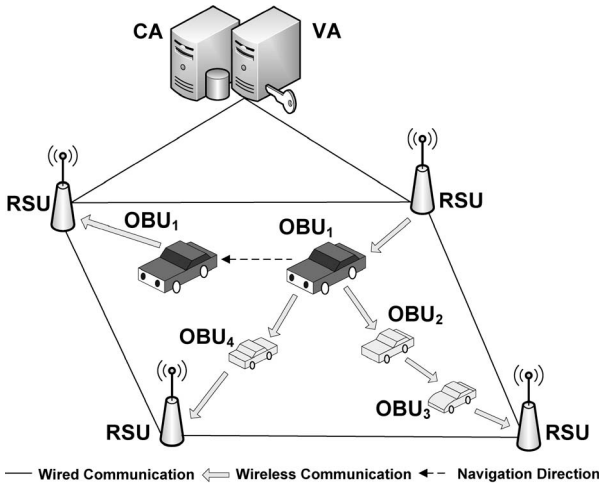


Fig. 1. VANET.

B. Threat and Trust Models

Vehicles are assumed to have constrained network transmission bandwidth but ample computation resources compared with typical mobile nodes [28], [29]. Therefore, we assume that vehicles are uncooperative to forward packets that are destined for other vehicles without compensation. To encourage cooperation, some rewards should be provided by the source vehicle (or even the destination vehicle) to intermediate vehicles. However, any introduction of remedy has its side effect. We assume that the drivers of some vehicles are greedy, trying to maximize their advantages but dodging responsibility. To be more specific, the following three actions could be carried out by these clever drivers.

1) *Credit fraudulence*. Greedy drivers will attempt to be rewarded for the work that they did not do or more than they have done.
2) *Sender repudiation*. Greedy drivers can either forge the credit claims or possibly steal the credit claims to achieve this goal.
3) *Driver collusion*. Greedy drivers might collude with each other if they can benefit from doing so.

For the trust models, the vehicles and RSUs fully trust CAs and VAs to perform secure-related transactions. RSUs can be treated as the extension of VAs to help with management things. They probe the network traffic and gather useful information back to VAs.

C. Goal Model

Because each vehicle has limited transmission and reception capabilities, two vehicles outside the transmission range of each other can only communicate through a sequence of intermediate vehicles in a multihop manner. Therefore, through intervehicle communication, our goal is to disseminate commercial advertisements over VANETs. This commercial campaign is also assumed to have spatial locality (within a certain area) and temporal locality (within a certain time interval).

The application scenario of advertisement dissemination is described as follows (see Fig. 2). When an advertisement provider would like to launch a commercial advertisement campaign over VANETs, he/she should first register with a VA to be granted the private key to distribute commercial advertisements. The VA will supervise the content, supplement advertisement information, and issue the relayer record. The relayer record

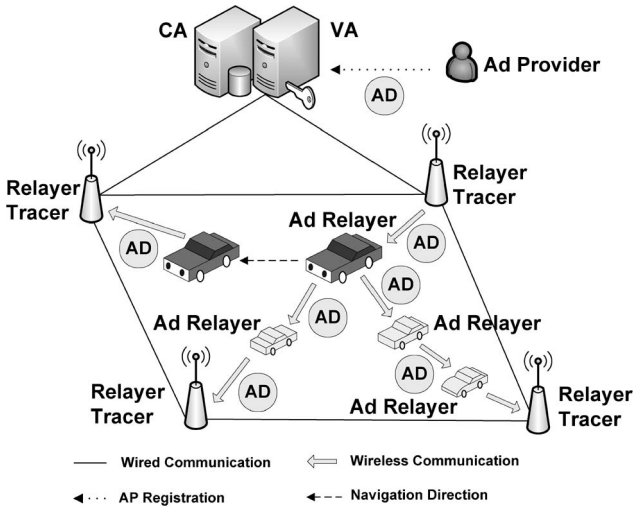


Fig. 2. Advertisement dissemination scenarios in VANETs.

contains the mixture of the private keys of the advertisement provider and the VA. Then, the VA appends the relayer record to the signed commercial advertisement and broadcasts to the network. When a vehicle, acting as an advertisement relayer, comes to help, the relayer first verifies the signature by the VA to check the integrity of the advertisement and inspects the advertisement information to avoid forwarding the same advertisement or forwarding the invalid advertisement.

Upon passing the verification, the relayer mingles its own private key with the mixed keys in the relayer record. After several hops of advertisement redistribution, VA-delegated RSUs, acting as relayer tracers, receive the relayer records from the broadcast channel and send to the VA to identify all the relayers in each relayer record. All VAs within one specific campaign region maintain a comprehensive record of the relayers. After the campaign calls to an end, the VA reports the list of relayers to the advertisement provider. Each of the relayers in the list will receive a voucher to buy some merchandise at a discount or even for free.

Because RSUs in VANETs cannot hear all the traffic, the relayer record for one specific advertisement campaign may not be complete. Some drivers would forward advertisements without compensation. In our scheme, the credit of one relayer is recorded not only in the relayer record that this relayer sends but also in all relayer records that originated in this relayer record. If any of the derived relayer records is received by RSUs, the credit will be counted. For more details, see Section V-B.

D. Payment Model

1) Parties and Relations: The payment model contains the following four basic parties:

a) the advertisement provider;
b) the advertisement relayer;
c) the store;
d) the VA.

The operations among these parties can be divided into the following three phases: 1) *certificate issuing*; 2) *payment*; and 3) *redemption*. In the *certificate issuing* phase, one advertisement provider has to register to the VA to be granted the privilege to disseminate commercial advertisements, whereas the advertisement relayer has to register to obtain its private key to join in the dissemination activity. Each advertisement relayer also has to provide the VA with a valid e-mail account to receive the personalized vouchers signed by the VA. In the *payment* phase, the corresponding expense of issued vouchers should be paid by the advertisement provider to the stores in advance to enable the exchange of merchandise by advertisement relayers. In the *redemption* phase, an advertisement relayer shows its voucher to the store. The store verifies the voucher and exchanges it for corresponding merchandise.

Our design relies only on a relatively tamper-proof secure module in each OBU. The OBU needs to store the private keys of its own and the system public parameters. In addition, the OBU performs simply the signature verification of the advertisement and the relayer record generation. Each OBU does not need to store the relayer record, because this information has been kept by surrounding RSUs every time that it relays. By using RSUs to maintain relayer information, we can greatly reduce the need for the tamper-proof secure module and lower the possibility of colluding among vehicles.

2) Charging and Rewarding Policy: Some solutions such as [17] consider that each vehicle has different forwarding cost and should be compensated according to individual costs. This design is ideal; however, it involves heavy computation and constant communication, which degrades the normal functionality of the networks. In addition, it stimulates collusion, because it can gain more benefits according to the floating rewarding policy. Therefore, we adopt the same rewarding rate for each advertisement relayed to keep the networks less affected and more efficient against uncooperative drivers.

Because the goal of our design is to disseminate commercial advertisements over a specific area and during a particular time interval, advertisements can efficiently be forwarded and flooded in one after the other. To be more specific, each advertisement carries information about its freshness (the sequence number) and validity (the valid time interval and geographical area). RSUs would periodically inject advertisements with corresponding information into VANETs. Based on this information, advertisement relayers can distinguish whether the advertisement has been forwarded. Advertisement relayers could also check this information before forwarding to avoid forwarding invalid advertisements. This way, relayers are always rewarded for their different relays and not just a fixed amount of compensation. Relayers can be provided with personalized vouchers, which are encrypted by the VA using the driver's public key, related to some particular products connected with the relayed advertisements. The vouchers are sent to the participating vehicles when VAs identify their participation. These vehicles can exchange merchandizes or have a discount when showing their personalized vouchers.

IV. Our Secure Incentive Scheme

Our construction is based on the RS-code [30]. For a large prime q and a positive integer δ, the RS-code $\mathrm{RS}(q, \delta)$ is a linear

code $C[n,k,d]$ with codeword length $n=q-1$, dimension $k=q-\delta$, and distance $d=\delta$. In addition, $t=\lfloor \delta-1/2 \rfloor$ is the maximal number of errors that could be corrected in the received word. Then, we can build one $k\times n$ generation matrix G and a corresponding $n\times(n-k)$ parity-check matrix H of C. The RS-code $\mathrm{RS}(q,\delta)$ is also a cyclic code over $\mathbb{Z}_q$ with generator $g(x)=\prod_{i=1}^{2t}(x-\alpha^i)$ of degree $2t$, where α is a primitive element of $(Z_q^*,\times)$, and $\delta-1=2t$. A message $m\in \mathbb{Z}_q^k$ is treated as a polynomial $m(x)$ of degree $k-1$, and the codeword of m can be expressed as $c(x)=m(x)g(x)$ of degree $n-1$ and dimension k. The codeword $c(x)$ has a factor of $g(x)$; therefore, it has roots $\alpha^1,\alpha^2,\ldots,\alpha^{2t}$. The parity-check matrix for $\mathrm{RS}(q,\delta)$ can then be written as

$$H_{n\times(n-k)}=\begin{bmatrix} (\alpha^1)^0 & (\alpha^2)^0 & \cdots & (\alpha^{2t})^0 \\ (\alpha^1)^1 & (\alpha^2)^1 & \cdots & (\alpha^{2t})^1 \\ (\alpha^1)^2 & (\alpha^2)^2 & \cdots & (\alpha^{2t})^2 \\ \vdots & \vdots & \ddots & \vdots \\ (\alpha^1)^{n-1} & (\alpha^2)^{n-1} & \cdots & (\alpha^{2t})^{n-1} \end{bmatrix}.$$

The Berlekamp–Massey algorithm [31] is a syndrome-based decoding algorithm for decoding RS-codes. When given a series of syndromes, we can find the error locator polynomial $\sigma(x)$ without finding the error magnitude. The fastest known algorithm so far is described in [32]. After the error locator polynomial has been decided, finding all of its roots is the next step. These roots denote the inverses of the error locations, which also represent the indices of the row vector in the parity-check matrix. In the past, Chien's search algorithm [33] was used to search all the possible roots. The Cantor–Zassenhaus algorithm [34] can work more efficiently with the expected running time, which corresponds to the square of the number of errors, compared to Chien's running time, which corresponds to the number of users. This number is also the number of the row vectors of the parity-check matrix of the RS-code.

In our design, the system has its own master key and issues each vehicle a respective private key. This private key is particularly used for advertisement dissemination rather than for general decryption or verification. Each participating vehicle's private key is associated with one row vector of the parity-check matrix Γ of one RS-code. The private key is one specific scalar multiplication of this row vector and therefore associates with one discrete logarithm representation problem, which will further be explained later.

The notations used throughout this paper are listed in Table I, followed by the principals involved in our scheme, as indicated in Table II. As shown in Fig. 3, the AP registers with the VA to be granted the private key to disseminate commercial advertisements. The AP first prepares the advertisement, and the VA inspects the content of the advertisement. Upon passing the inspection, this advertisement is signed by the VA and appended one relayer record (RR) that consists of the mixture of the private keys of the VA and this AP. When the advertisement relayer (AR) comes to help, he/she just mingles his/her private key with the mixed ones in the RR of the commercial advertisement. After several hops of relaying, RTs along the road receive RRs from the broadcast channel. RTs identify all the ARs that have participated in the advertisement relaying process, given that the number of the ARs is not over the predefined maximal number of errors of the RS-code. RTs then report their own relayer lists to the VA of their administrative domain, and the VA produces an accumulated relayer list. Finally, the VA sends this relayer list to the AP, and the AP rewards the ARs according to their respective contributions.

To describe our scheme, we need the following definitions.

Definition 1—Representations: Our secure incentive scheme relies on the representation problem. When $y=\prod_{i=1}^{2t}h_i^{\delta_i}$, $(\delta_1,\ldots,\delta_{2t})$ is said to be a representation of y with respect to the base $h_1,\ldots,h_{2t}$.

TABLE I
NOTATIONS

Notation	Descriptions
$\mathrm{RS}(q,\delta)$	Reed-Solomon code with argument q and δ
H	Parity-check matrix of a linear code
Γ	Finite field of q elements
$\sigma(x)$	Error locator polynomial of a received word
h_i	i-th element of the base of a representation
$(\delta_1,...,\delta_{2t})$	Representation with respect to the base $h_1,...,h_{2t}$
$\overline{d}$	Representation with respect to the base $h_1,...,h_{2t}$
G_q	Multiplicative subgroup of a finite field of size q
RR	Relayer Record
AD	Advertisement

TABLE II
PRINCIPALS IN OUR INCENTIVE SCHEME

Principal	Description
CA	Certificate Authority
VA	Vehicular Authority
AP	Advertisement Provider
AR	Advertisement Relayer
RT	Relayer Tracer

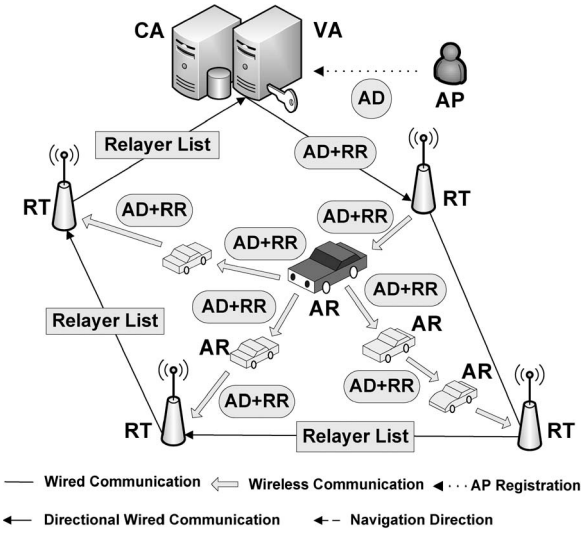


Fig. 3. Advertisement dissemination scenario of our design.

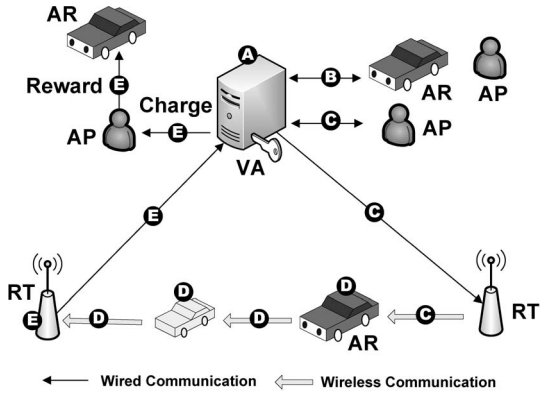


Fig. 4. Design of the proposed incentive scheme.

Definition 2—Convex Combination: If $\overline{d}_1, \ldots, \overline{d}_m$ are representations of y with respect to the base $h_1, \ldots, h_{2t}$, any convex combination of these representations also yields the representation of y, i.e., $\overline{d} = \sum_{i=1}^{m} \alpha_i \overline{d}_i$ is the representation of y, where $\sum_{i=1}^{m} \alpha_i = 1$.

The security of our incentive scheme relies on the discrete logarithm representation problem defined as follows.

Definition 3—Discrete Logarithm Representations Problem: For y, $h_1, \ldots, h_{2t} \in G_q$, and $\overline{d}_1, \ldots, \overline{d}_m$, the representations of y with respect to the base $h_1, \ldots, h_{2t}$, the discrete logarithm representation problem is to construct a representation $\overline{d}$ of y, where $\overline{d}$ is not a convex combination of $\overline{d}_1, \ldots, \overline{d}_m$.

Our incentive scheme is designed as shown in Fig. 4. The scheme consists of the following five phases:

1) initialization;
2) private key generation;
3) advertisement generation and publishing;
4) Advertisement (AD) relaying and RR update;
5) RTs tracing.

A. Initialization (Involving the VA)

This phase contains the following three steps.

1) The VA decides N and t such that the system could support at most N users, and each advertisement is relayed through at most t hops. Then, the VA generates one RS-code RS(q, δ), where $q \geq N$, and $\delta \geq 2t + 5$. In addition, the VA calculates the corresponding parity-check matrix H. Let Γ be the parity check matrix of RS(q, δ). Express Γ as follows:

$$\Gamma = \begin{bmatrix} \gamma^{(0)} \\ \gamma^{(1)} \\ \vdots \\ \gamma^{(n-1)} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \gamma_1^{(1)} & \gamma_2^{(1)} & \cdots & \gamma_{2t}^{(1)} \\ \gamma_1^{(2)} & \gamma_2^{(2)} & \cdots & \gamma_{2t}^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_1^{(n-1)} & \gamma_2^{(n-1)} & \cdots & \gamma_{2t}^{(n-1)} \end{bmatrix}.$$

2) Let $g \in G_q$ be a generator of G_q. The VA chooses random $r_i \in \mathbb{Z}_q$ and computes $h_i = g^{r_i}$ for $i = 1, \ldots, 2t$.
3) The VA chooses random α_i for $i = 1, \ldots, 2t$ and computes $y = \prod_{i=1}^{2t} h_i^{\alpha_i}$. Treat $\langle y, h_1, \ldots, h_{2t} \rangle$ as public information, which can be protected by the VA's digital signature.

B. Private Key Generation (Involving the AP/AR and the VA)

This phase contains the following four steps.

1) The AR registers with the VA by showing its public-key certificate. The VA then launches a challenge-response authentication mechanism by encrypting nonce using the public key specified in this certificate. If the AR could respond with the correct nonce, it is authorized the private key for ad relaying. The AP follows the same procedure as what the AR does to be granted the private key for ad provision.
2) The VA computes $\theta_i \in \mathbb{Z}_q$ of the AR/AP with ID$_i$ using the ith row of Γ such that $\overline{d}_i = \theta_i \cdot \gamma^{(i)}$ is a representation of y with respect to the base $h_1, \ldots, h_{2t}$, where $\gamma^{(i)} = (\gamma_1^{(i)}, \ldots, \gamma_{2t}^{(i)}) \in \Gamma$, i.e.,

$$\theta_i = \left(\sum_{j=1}^{2t} \gamma_j^{(i)} \alpha_j \right) \Big/ \left(\sum_{j=1}^{2t} \gamma_j^{(i)} r_j \right) \pmod{q}.$$

3) $\overline{d}_i$ is the private key of the AR/AP with ID$_i$ for ad relaying or providing.
4) The private key can be protected by the VA's digital signature and securely sent to the AR/AP.

C. AD Generation and Publishing (Involving the AP, the VA, and RSUs)

This phase contains the following four steps.

1) The AP shows the VA the intended AD and its own private key previously signed by the VA for ad provision.
2) The VA verifies whether the content of the intended AD is appropriate and the signature on the private key is intact. If not, drop this request; otherwise, go to step 3.
3) The VA chooses random α_1, $\alpha_2 = 1 - \alpha_1 \pmod{q}$, and computes the RR as the convex combination $\overline{d} = \alpha_1 \overline{d}_{VA} + \alpha_2 \overline{d}_{AP}$.
4) The VA asks nearby RSUs to periodically broadcast the signed AD together with its RR $\overline{d}$ The signed AD includes the AD's information, such as the sequence number, the valid campaign geographical range, and the valid time interval.

D. AD Relaying and RR Update (Involving the AR)

This phase contains the following four steps.

1) The AR verifies the signed AD through the VA's digital signature and decides whether to forward this AD based on the information embedded in the AD.

2) The AR calls the received RR $\overline{d}$ and verifies whether $\overline{d}$ is the representation of y. If not, drop this RR; otherwise, go to step 3.
3) The AR chooses random α_1, $\alpha_2 = 1 - \alpha_1 \pmod q$, and computes the convex combination of $\overline{d}$ and its private key $\overline{d}_i$ as $\overline{d}' = \alpha_1 \overline{d} + \alpha_2 \overline{d}_i$.
4) The AR broadcasts the signed AD together with the updated RR $\overline{d}'$. The signed AD is embedded with related information.

E. RTs Tracing (Involving the RT and the VA)

This phase contains the following three steps.

1) Because each RR contains the syndrome of the RS-code, one RT runs the Berlekamp–Massey algorithm on the received RR to calculate the error locator polynomial $\sigma(x)$ and runs the Cantor–Zassenhaus algorithm to determine all the roots that represent the error location numbers, i.e., the indices of the ARs. Most importantly, the existence of the AP's and the VA's indices indicates the validity of this RR.
2) RTs then report their own relayer lists to the VA of their administrative domain, and the VA produces an accumulated relayer list.
3) The VA sends the AR list to the AP, and the AP rewards the ARs according to their respective contributions.

V. Security Analysis and Performance Evaluation

In this section, we first analyze the correctness and security of our scheme by giving formal arguments. Next, we compare our scheme with the representation signature-based and voucher-based schemes. We further evaluate the correctness of our construction in the real-world scenario that RSUs may not hear all the traffic in VANETs.

A. Security Analysis

We first explain the correctness of our incentive design. For the relayer record, any convex combination of some representations of y with respect to one base is also the representation of y with respect to this base. Any driver can first verify whether the received relayer record is the representation of y, because there could be some drivers who try to destruct the relayer record by blending in some invalid private key information. In addition, one vehicle can perform one convex combination by summing up the weighted relayer record and its private key to be later identified as a relayer. The following theorem states the aforementioned properties.

Theorem 1—Correctness: If $\overline{d}_1, \ldots, \overline{d}_m$ are representations of y with respect to the base $h_1, \ldots, h_{2t}$, any convex combination of these representations also yields the representation of y, i.e., $\overline{d} = \sum_{i=1}^{m} \alpha_i \overline{d}_i$ is the representation of y, where $\sum_{i=1}^{m} \alpha_i = 1$.

Proof: By definition, $\overline{d}_i = (\delta_{i,1}, \ldots, \delta_{i,2t})$, $y = \prod_{j=1}^{2t} h_j^{\delta_{i,j}}$ for $1 \le i \le m$. In addition, $\sum_{i=1}^{m} \alpha_i = 1$. We have

$$\begin{aligned} \because\ \overline{d} &= \sum_{i=1}^{m} \alpha_i \overline{d}_i = \sum_{i=1}^{m} (\alpha_i(\delta_{i,1}, \ldots, \delta_{i,2t})) \\ &= \left(\sum_{i=1}^{m} \alpha_i \delta_{i,1}, \ldots, \sum_{i=1}^{m} \alpha_i \delta_{i,2t} \right). \\ \therefore\ \prod_{j=1}^{2t} h_j^{\sum_{i=1}^{m} \alpha_i \delta_{i,j}} &= \prod_{i=1}^{m} \left(\prod_{j=1}^{2t} h_j^{\delta_{i,j}} \right)^{\alpha_i} \\ &= \prod_{i=1}^{m} y^{\alpha_i} = y^{\sum_{i=1}^{m} \alpha_i} = y. \end{aligned}$$

Therefore, $\overline{d}$ is the representation of y. ■

The security of our incentive scheme relies on the discrete logarithm representation problem. In Section III-C, clever drivers would carry out *credit fraudulence attacks* to gain more advantages. For one legitimate driver who possesses a private key pair for ad relaying, he/she fails to construct a valid RR that contains the VA's and the AP's private keys. As described in Section IV-C, the RR contains the mixture of private keys of both the VA and the AP. He/She has to find the VA's and the AP's private keys to forge a new RR. All that he/she can do is to solve the discrete logarithm representation problem, because finding one specific private key within one RR can be reduced to solving the *discrete logarithm problem* (DLP) in G_q.

On the other hand, the AP also tries to avoid being charged when launching *sender repudiation attacks*. The AP would try to remove its own contribution to the RR to repudiate his expense. What the AP can do is solve the discrete logarithm representation problem and remove its contribution to the RR. However, this method is also not possible, assuming that the DLP is hard in G_q. The following theorem formalizes the aforementioned scenarios.

Theorem 2—Security: Let $\langle y, h_1, \ldots, h_{2t} \rangle$ be the public information. If one adversary can generate a new representation $\overline{d}$ of y with respect to $h_1, \ldots, h_{2t}$, which is not a convex combination of $\overline{d}_1, \ldots, \overline{d}_m$, then the adversary can compute a discrete logarithm in G_q, i.e., the convex combination is the only representation of y that can efficiently be constructed when given $\overline{d}_1, \ldots, \overline{d}_m \in \mathbb{Z}_q^{2t}$, assuming the difficulty of the DLP in G_q.

Proof: Given g, $z \in G_q$, where $z = g^x$, find x. First, randomly choose $a, b, r = (r_1, \ldots, r_m)$, $s = (s_1, \ldots, s_{2t})$, where each scalar is in $\mathbb{Z}_q$. Then, construct the representation base $h_1, \ldots, h_{2t}$, where

$$h_i = \begin{cases} z^{r_i} g^{s_i}, & 1 \le i \le m \\ g^{s_i}, & m+1 \le i \le 2t. \end{cases}$$

Let $y = z^a g^b = g^{ax+b}$. Find m linearly independent solutions $\alpha_1, \ldots, \alpha_m$ such that $\alpha_i \cdot r = a \pmod q$ and extend $\alpha_1, \ldots, \alpha_m$ to $\alpha'_1, \ldots, \alpha'_m$ while keeping α'_i's first m entries unchanged such that $\alpha'_i \cdot s = b \pmod q$, where α'_i are the representations of y. Find β, which is the representation of y but not a convex combination of $\alpha'_1, \ldots, \alpha'_m$ such that

$\beta \cdot r = a' \neq a \pmod q$, and then, $a'x + \beta \cdot s = ax + b$, $x = (\beta \cdot s - b)(\alpha - \alpha')^{-1} \pmod q$.

For the *driver's collusion attack*, the number of credits with which one vehicle can be rewarded for one specific advertisement is fixed, as mentioned in Section III-D2. Because our scheme utilizes the RS-code, each vehicle that contributes to the RR can uniquely be identified. This identification corresponds to finding the error locations of one received word. Each vehicle can only be identified once for forwarding one specific advertisement, i.e., they will be rewarded for one time for each advertisement with the same information. Any interested vehicles could help disseminate different advertisements and be rewarded corresponding credits for their works. Because no extra credits are given to the colluding different vehicles, drivers cannot benefit from colluding.

B. Computation and Communication Analysis

In this section, the following three representative schemes are compared: 1) the signature-based scheme [20]; 2) the voucher-based scheme [21]; and our (record-based) scheme.

We assume that there are n vehicles and K maximal number of vehicles that participate in relaying commercial advertisements. First, the VA has to decide N and K such that the system could support at most N vehicles and that each advertisement is relayed through at most K hops/relayers.

Assume that the number of vehicles N is one million (10^6) and the maximal number of hops/relayers for one advertisement is K. The parameters are given as follows: q is at least 160 b long. For the overall message generated, if at most K ARs together with the VA and the AP are in the record, the relayer record contains $(d-1) = 2(K+2)$ elements of length 160 b. On the other hand, if the voucher-based scheme adopts the *elliptic-curve digital signature algorithm* (ECDSA), the total message size is about 196 KB, where 112 B is the size of one receipt and its corresponding signature, and 84 B is the size of one onion voucher. Finally, the signature-based scheme also adopts ECDSA, and the total message size is about 112 KB.

For the storage size, the vehicle in the voucher-based scheme needs to store all the receipts and vouchers and hand over to the authorities, whereas the vehicles in the signature-based scheme and our scheme do not need to store anything. For the communication complexity, the voucher-based scheme requires three-way handshaking, which is the heaviest load among these three schemes. The first message size is 120 B, whereas the second message size is 84 KB. For the signature-based scheme, only one broadcast communication is needed; the message size is 112 KB, where K is the number of relayers that contribute to relaying this message. For our scheme, one broadcast communication is needed; the message size is $2(K+2) \cdot 20$ B. Our scheme outperforms the other two schemes by a factor of 2–3, which is a great reduction for the relayers and the traffic in VANETs.

For the computation complexity, the signature- and the voucher-based schemes need complex ECDSA signature generation, whereas our scheme needs only a simple linear combination of two vectors. This condition implies faster processing of relayer records and forwarding of the corresponding commercial advertisement (see Table III).

TABLE III
COMPUTATION AND COMMUNICATION ANALYSIS (FOR EACH AR)

$N = 10^6$	Signature [20]	Voucher [21]	Our Scheme
Storage Size (B)	0	$196K + 28$	0
Communication Size (B)	$112K$	$84K$	$40(K+2)$
Communication Link	1 broadcast	1 broadcast 1 unicast	1 broadcast
Computation Operation	ECDSA signature generation	ECDSA signature generation	convex combination (of two vectors)

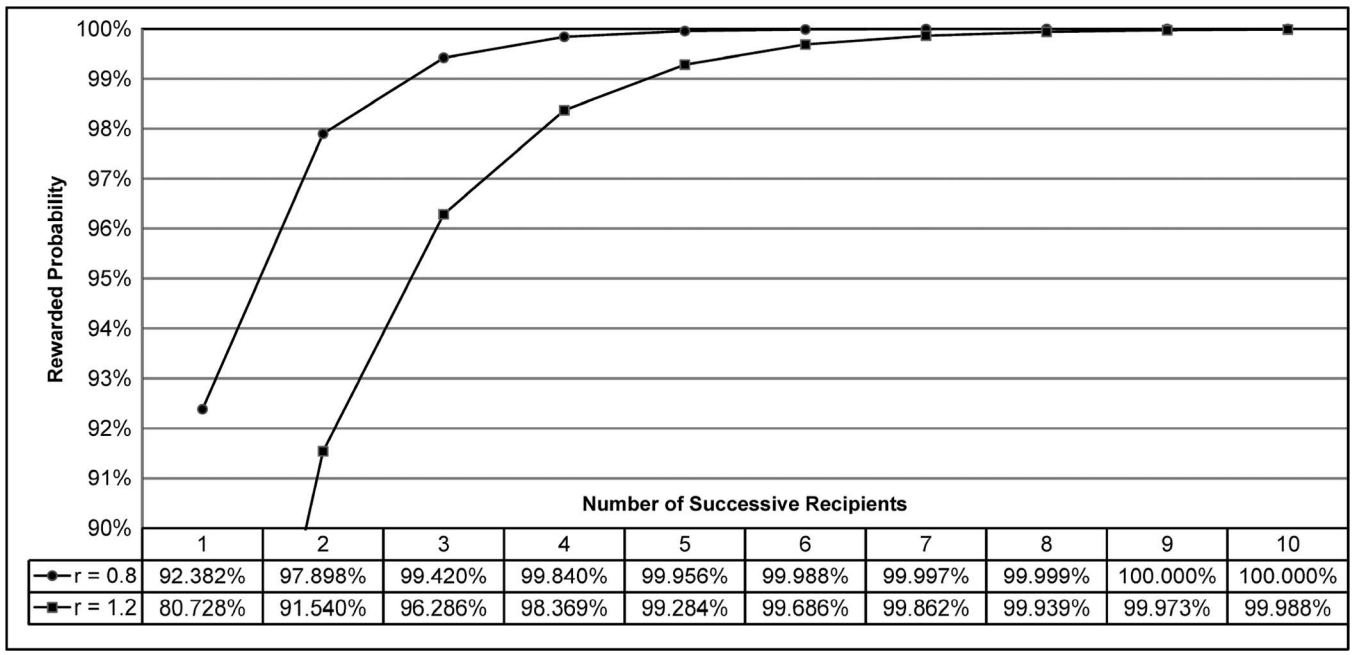
TABLE IV
COMPUTATION AND COMMUNICATION ANALYSIS ($K = 20$)

$N = 10^6$, $K = 20$	Signature [20]	Voucher [21]	Our Scheme
Communication Overhead	2.24kB	1.8kB	0.88kB
Storage Overhead	0kB	196kB	0kB

Based on the developing standards in *Dedicated Short-Range Communications* (DSRC) and IEEE 802.11p [34]–[36], a vehicle can achieve a nominal transmission range of 300 m (up to 1000 m) while moving at a speed up to 120 mi/h. The default data rate is 6 Mb/s (up to 27 Mb/s). We assume that K is 20 and the transmission time can be omitted; therefore, the largest area that the vehicles can cover is a circle with a radius of 20 km (i.e., 1200 km^2), assuming that the number of hops/relayers for one advertisement is 20 (i.e., $K = 20$). The number of RSUs deployed is about 3000 [37]. The real-world deployment overhead of different schemes is provided in Table IV.

Based on the RSU placement scheme [37]–[39], we can conclude that the disconnection interval could be shorter if RSUs are deployed in an overlap manner and usually in the intersections. It is pointed out that, if the communication range is 300 m and the overlap ratio is 0.8, the connectivity can reach up to 72.4% for an area of size about 1000 km^2. On the other hand, the disconnection interval is shorter than 7 s with the same parameters. If the vehicle moves at a speed of 70 km/h, the expected interval of connectivity is 130 m, i.e., the vehicle can contact with RSUs within 130 m. In addition, the commercial campaign is usually timing sensitive, and therefore, VAs issue the same advertisement with a timestamp on it. This mechanism can further reduce the relayer allocation of a RS-code, because RSUs can further process broadcast advertisements when the number of expected ARs is small.

For the possibility of the incomplete RR, our design shows that there is only slight chance that one AR forwarded ADs without compensation. The credit of one AR is recorded not only in the RR that this AR sends but in all RRs that originated in this RR as well. If any of the derived RRs is received by RSUs, the credit will be counted. We use the deployment scheme in [37], and their results showed that, if the overlap



	1	2	3	4	5	6	7	8	9	10
r = 0.8	92.382%	97.898%	99.420%	99.840%	99.956%	99.988%	99.997%	99.999%	100.000%	100.000%
r = 1.2	80.728%	91.540%	96.286%	98.369%	99.284%	99.686%	99.862%	99.939%	99.973%	99.988%

Fig. 5. Rewarded probability to the number of successive recipients.

ratio of the RSU is 0.8, the probability of disconnection of the OBU is 27.6%. Therefore, if one AR Bob receives the RR from the AR Alice, the probability that Alice can get compensation is about 92.4%, which means that at least one of the RRs from these two ARs reaches RSUs. In addition, Alice can get compensation for the services in more than 99 out of 100 times when there are more than two ARs that receive the RR that originated in her. The probability is more than 99.99% when the RR that originated in Alice is heard by at least seven succeeding ARs.

On the other hand, they [37] also worked on the overlap ratio 1.2, and the corresponding disconnection probability was 43.9%. For this sparser deployment, the rewarding probability is still more than 99%, given that there are at least five successive relayers that receive the RR that originated in Alice. See Fig. 5 for further results.

C. Extended Scheme

Inherent from the tracing ability of RS-codes, the maximal number of errors corrected is fixed. However, by using the algorithm introduced by Guruswami and Sudan [40], [41], we can list candidate codewords for the received word containing more than K errors (up to $2K-1$). In addition, for the errors equal to or larger than $2K$, the tracing amendment is provided in [27].

To provide a variant of our design, the AP could reward ARs according to different contributions. Each OBU can be preloaded with several private keys for advertisement dissemination [42]. If the same advertisement is encountered, the OBU can use different ad-relaying private keys of its own to be identified later by the VA. The AP can provide different rewards according to the number of AR's relays.

To enhance the authenticity of an advertisement and related relayer record, the VA could select a private key of the AP by the critical information of the advertisement such as the provider name, the duration of the commercial campaign, and the valid dissemination area. The hashed value of the critical information is used to decide which row of the parity-check matrix of the RS-code is selected as the private key for this specific advertisement. This further consideration provides strong binding between the advertisement and its corresponding relayer record.

VI. Conclusion

We have proposed a secure and practical incentive scheme for commercial advertisement dissemination over VANETs. Our contributions are the following four points.

1) *All* cooperative vehicles are rewarded with incentives, whereas the uncooperative cannot gain *any* advantage by the correctness and security proof.
2) Cooperative vehicles can be identified within one single operation over the relayer record by using the decoding algorithm of RS-codes.
3) The size of relayer records is constant to the number of predefined relayers for one advertisement rather than proportional to the total number of cooperative vehicles.
4) The number of communication between vehicles is minimized to one single broadcast (or Geocast) communication, and no interaction between vehicles is needed.

With careful design and analysis, our scheme encourages cooperation among vehicles by providing secure incentives. We also made comparisons with the previous works and conclude that our scheme is robust in terms of security and also cost effective in terms of communication and computation. In future work, we would like to further refine the tracing algorithm to speed up the tracing performance and generate more promising applications over VANETs.

REFERENCES

[1] H. Hartenstein and K. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 6, pp. 164–171, Jun. 2008.

[2] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[3] T. Nadeem, S. Dashtinezhad, C. Liao, and L. Iftode, "Trafficview: Traffic data dissemination using car-to-car communication," *SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 8, no. 3, pp. 6–19, Jul. 2004. [Online]. Available: http://doi.acm.org/10.1145/1031483.1031487

[4] M. D. Dikaiakos, S. Iqbal, T. Nadeem, and L. Iftode, "VITP: An information transfer protocol for vehicular computing," in *Proc. 2nd ACM Int. Workshop VANET*, 2005, pp. 30–39.

[5] V. Gradinescu, C. Gorgorin, R. Diaconescu, V. Cristea, and L. Iftode, "Adaptive traffic lights using car-to-car communication," in *Proc. IEEE 65th VTC—Spring*, Apr. 2007, pp. 21–25.

[6] J. Rybicki, B. Scheuermann, W. Kiess, C. Lochert, P. Fallahi, and M. Mauve, "Challenge: Peers on wheels—A road to new traffic information systems," in *Proc. 13th Annu. ACM Int. Conf. MobiCom*, 2007, pp. 215–221.

[7] J. Yoon, B. Noble, and M. Liu, "Surface street traffic estimation," in *Proc. 5th Int. Conf. MobiSys*, 2007, pp. 220–232.

[8] C. Li and S. Shimamoto, "An open traffic light control model for reducing vehicles CO2 emissions based on ETC vehicles," *IEEE Trans. Veh. Technol.*, 2011, DOI: 10.1109/TVT.2011.2168836.

[9] M. Guo, M. Ammar, and E. Zegura, "V3: A vehicle-to-vehicle live video streaming architecture," in *Proc. 3rd IEEE Int. Conf. PerCom*, Mar. 2005, pp. 171–180.

[10] U. Lee, J. Lee, J.-S. Park, and M. Gerla, "Fleanet: A virtual market place on vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 1, pp. 344–355, Jan. 2010.

[11] L. Zhou, Y. Zhang, K. Song, W. Jing, and A. Vasilakos, "Distributed media services in P2P-based vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 692–703, Feb. 2011.

[12] M. Caliskan, D. Graupner, and M. Mauve, "Decentralized discovery of free parking places," in *Proc. 3rd Int. Workshop VANET*, 2006, pp. 30–39.

[13] A. Nandan, S. Tewari, S. Das, M. Gerla, and L. Kleinrock, "AdTorrent: Delivering location cognizant advertisements to car networks," in *Proc. IEEE/IFIP WONS*, Les Menuires, France, Jan. 2006.

[14] S. Smaldone, L. Han, P. Shankar, and L. Iftode, "Roadspeak: Enabling voice chat on roadways using vehicular social networks," in *Proc. 1st Workshop SocialNets*, 2008, pp. 43–48.

[15] R. Lu, X. Lin, H. Zhu, and X. Shen, "An intelligent secure and privacy-preserving parking scheme through vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 6, pp. 2772–2785, Jul. 2010.

[16] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *IEEE Veh. Technol. Mag.*, vol. 2, no. 2, pp. 12–22, Jun. 2007.

[17] F. Li and J. Wu, "Frame: An innovative incentive scheme in vehicular networks," in *Proc. IEEE ICC*, Jun. 2009, pp. 1–6.

[18] M. Mahmoud and X. Shen, "PIS: A practical incentive system for multihop wireless networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 4012–4025, Oct. 2010.

[19] B. Lamparter, K. Paul, and D. Westhoff, "Charging support for ad hoc stub networks," *Comput. Commun.*, vol. 26, no. 13, pp. 1504–1514, Aug. 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366403000343

[20] J. P. Jayapalan and S. D. Magee, "Method and system for providing credit for participation in an ad hoc network," U.S. Patent 20 070 230 438, Oct. 4, 2007. [Online]. Available: http://www.freepatentsonline.com/2007/0230438.html.

[21] S.-B. Lee, G. Pan, J.-S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," in *Proc. 8th ACM Int. Symp. MobiHoc*, 2007, pp. 150–159.

[22] H. Janzadeh, K. Fayazbakhsh, M. Dehghan, and M. S. Fallah, "A secure credit-based cooperation stimulating mechanism for manets using hash chains," *Future Gener. Comput. Syst.*, vol. 25, no. 8, pp. 926–934, Sep. 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X08001969

[23] T. Chen and S. Zhong, "INPAC: An enforceable incentive scheme for wireless networks using network coding," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[24] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," CoRR, vol. cs.NI/03070122003.

[25] Q. He, D. Wu, and P. Khosla, "A secure incentive architecture for ad hoc networks," *Wireless Commun. Mobile Comput.*, vol. 6, no. 3, pp. 333–346, May 2006. [Online]. Available: http://dx.doi.org/10.1002/wcm.399

[26] D. Boneh and M. Franklin, "An efficient public key traitor tracing scheme," in *Proc. CRYPTO*, vol. 1666, 1999, p. 783. [Online]. Available: http://dx.doi.org/10.1007/3-540-48405-1_22

[27] P. Junod, A. Karlov, and A. Lenstra, "Improving the Boneh–Franklin traitor tracing scheme," in *Proc. PKC*, vol. 5443, 2009, pp. 88–104. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-00468-1_6

[28] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[29] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Implementation, performance, and research challenges," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 110–118, Nov. 2008.

[30] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *J. Soc. Ind. Appl. Math.*, vol. 8, no. 2, pp. 300–304, 1960. [Online]. Available: http://link.aip.org/link/?SMM/8/300/1

[31] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, vol. IT-15, no. 1, pp. 122–127, Jan. 1969.

[32] V. Y. Pan, "Faster solution of the key equation for decoding BCH error-correcting codes," in *Proc. 29th Annu. ACM STOC*, 1997, pp. 168–175.

[33] R. Chien, "Cyclic decoding procedures for Bose–Chaudhuri–Hocquenghem codes," *IEEE Trans. Inf. Theory*, vol. IT-10, no. 4, pp. 357–363, Oct. 1964.

[34] D. G. Cantor and H. Zassenhaus, "A new algorithm for factoring polynomials over finite fields," *Math. Comput.*, vol. 36, no. 154, pp. 587–592, Apr. 1981. [Online]. Available: http://www.jstor.org/stable/2007663

[35] *Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems—5-GHz-Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ASTM E2213-03, Sep. 2003.

[36] *IEEE 802.11 Working Group of the IEEE 802 Committee*, IEEE P802.11p/D10.0, Jan. 2010.

[37] Y. Sun, X. Lin, R. Lu, X. Shen, and J. Su, "Roadside units deployment for efficient short-time certificate updating in VANETs," in *Proc. IEEE ICC*, May 2010, pp. 1–5.

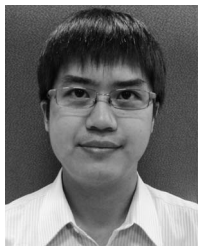
[38] W. Chen and S. Cai, "Ad hoc peer-to-peer network architecture for vehicle safety communications," *IEEE Commun. Mag.*, vol. 43, no. 4, pp. 100–107, Apr. 2005.

[39] J. Lee and C. Kim, "A roadside unit placement scheme for vehicular telematics networks," in *Proc. Adv. Comput. Sci. Inf. Technol.*, vol. 6059, 2010, pp. 196–202. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-13577-4_17

[40] V. Guruswami and M. Sudan, "Improved decoding of Reed–Solomon and algebraic-geometric codes," in *Proc. Annu. IEEE Symp. Found. Comput. Sci.*, 1998, pp. 28–37.

[41] V. Guruswami, "Improved decoding of Reed–Solomon and algebraic-geometry codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1757–1767, Sep. 1999. [Online]. Available: http://ci.nii.ac.jp/naid/80011295741/en/

[42] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.



Fu-Kuo Tseng received the B.S. and M.S. degrees in 2006 and 2008, respectively, from the National Chiao Tung University, Hsinchu, Taiwan, where he is currently working toward the Ph.D. degree with the Department of Computer Science.

His research interests include applied cryptography, network security, coding theory, and algorithm design in wireless sensor and mobile ad hoc networks, particularly in vehicular environments.

Yung-Hsiang Liu received the B.S. and M.S. degrees in 2006 and 2008, respectively, from the National Chiao Tung University, Hsinchu, Taiwan, where he is currently working toward the Ph.D. degree with the Department of Computer Science.

His research interests include network security, coding theory, and cryptography, particularly in pairing-based cryptosystems and secret-sharing schemes.

Jing-Shyang Hwu received the B.S., M.S., and Ph.D. degrees in computer science from the National Chiao Tung University, Hsinchu, Taiwan, in 1996, 1998, and 2005, respectively.

He is currently the deputy technical manager with the ICT Design and Validation for Vehicles Department, Telematics and Vehicular Control System Division, Information and Communications Research Laboratory, Industrial Technology Research Institute, Hsinchu. His research interests include wireless access in vehicular environments (WAVE)/dedicated short-range communications (DSRC) standard and protocol design, and vehicular ad hoc network (VANET) security and privacy.

Rong-Jaye Chen received the B.S. degree in mathematics from the National Tsing Hua University, Hsinchu, Taiwan, in 1977 and the Ph.D. degree in computer science from the University of Wisconsin, Madison, in 1987.

He is currently a Professor with the Department of Computer Science, National Chiao Tung University, Hsinchu. His research interests include cryptography, coding theory, algorithm design, and theory of computation.