SIRC: A Secure Incentive Scheme for Reliable Cooperative Downloading in Highway VANETs

Chengzhe Lai, *Member, IEEE*, Kuan Zhang, *Student Member, IEEE*, Nan Cheng, *Student Member, IEEE*, Hui Li, *Member, IEEE*, and Xuemin Shen, *Fellow, IEEE*

***Abstract*— In this paper, we propose a secure incentive scheme to achieve fair and reliable cooperative (SIRC) downloading in highway vehicular ad hoc networks (VANETs). SIRC can stimulate vehicle users to help download-and-forward packets for each other and consists of cooperative downloading and forwarding phase. During the cooperative downloading phase, SIRC utilizes "virtual checks" associated with the designated verifier signature to ensure fair and secure cooperation. Meanwhile, to minimize the payment risk of the client vehicle, partial prepayment strategy is adopted, i.e., the vehicles involved in downloading packets can only obtain part of the check before the client vehicle confirms the packet reception. During the cooperative forwarding phase, a profit-sharing model associated with an aggregating Camenisch–Lysyanskaya (CL) signature can stimulate cooperation and reduce the authentication overhead. In addition, we develop a reputation system to encourage cooperation and punish malicious vehicles. The aggregating CL signature and the symmetric cryptosystem are applied to resist various attacks, including injection/removing attack, free riding attack, submission refusal attack, and denial of service attacks. Extensive simulation results are given to show that the proposed SIRC can achieve a high download success rate and low average download delay with moderate cryptographic computation and communication overhead.**

***Index Terms*— VANET, incentive, cooperation, security, downloading, drive-thru Internet.**

I. Introduction

VEHICULAR Ad-Hoc Networks (VANETs) integrate telecommunication and informatics technologies into the transportation system, which features information gathering, processing, computing and transmission, and enables the evolution to next generation intelligent transportation systems (ITSs) [1]–[4]. In ITSs, a variety of emerging multimedia applications, e.g., video streaming, social networking, etc., can be delivered to passengers via VANETs to make their trips more convenient and enjoyable, especially during a long highway journey. VANETs currently support the interactions of vehicle-to-vehicle (V2V), vehicle-to-road infrastructure (V2R), and vehicle-to-Internet (V2I). For V2I, cellular and WiFi are two promising candidates. Vehicles can communicate with the cellular network or Roadside Units (RSUs) for the Internet access [5]. Although the cellular network is the most common method for vehicular Internet access due to its ubiquitous coverage, it is prohibitively costly for downloading bulk data, such as video clips, movie tailors. Moreover, cellular networks are currently facing severe traffic overload problems caused by excessive mobile data demands.

Offloading a portion of the cellular traffic through other types of networks is a promising solution [6]. Particularly, in VANETs, vehicles can download data from RSUs with high bandwidth and low cost instead of directly from the cellular network. The Internet access provided by RSUs to passing-by vehicles is referred to as the drive-thru Internet [7], which has recently drawn overwhelming attention from both academia and the automobile industry. In spite of the high data rate, drive-thru Internet suffers the short and intermittent connections due to the high mobility of vehicles. For example, a general drive-thru connection at the speed of 80 km/h lasts about 20 s, which in turn can transfer only 9 MB data [8]. In addition, due to the limited number of RSUs deployed in the sparse highway, it is difficult to provide ubiquitous access all the time. Therefore, the cooperative downloading in highway VANETs, i.e., each vehicle helps download part of a file for a target vehicle, is necessary [9]–[11], especially when large files are requested.

To reliably, fairly and securely achieve the cooperative downloading, several research issues should be addressed. Firstly, due to the intermittent connections in VANETs, the cooperative downloading delay is high. Since vehicles may exit the highway, it is crucial to deliver the complete file (especially the large ones) in a timely manner. In addition, vehicle users may not be willing to spend their limited resources, such as battery energy, computing capability and available network bandwidth, to help others download and relay packets without compensation. Even though some vehicle users are motivated by interests, they may also behave selfishly and maliciously. For instance, they probably deny or

Manuscript received December 7, 2015; revised May 23, 2016 and September 1, 2016; accepted September 17, 2016. This work was supported by the National Natural Science Foundation of China Research under Grants 61502386, 61472472, 61402366, and U1401251, and by the International Science and Technology Cooperation and Exchange Plan in Shaanxi Province of China under Grant 2015KW-010. The Associate Editor for this paper was L. Yang.

C. Lai is with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China, and also with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China (e-mail: lcz.xidian@gmail.com).

K. Zhang, N. Cheng, and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: k52zhang@uwaterloo.ca; n5cheng@uwaterloo.ca; ssheng@uwaterloo.ca).

H. Li is with the State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China (e-mail: lihui@mail.xidian.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TITS.2016.2612233

refuse to help download and relay packets although they have obtained the credits provided by the target vehicle. In addition, some malicious vehicle users may intentionally modify or drop packets in a hardly detected way. On the other hand, the vehicles involved in helping download and forward the packets may not obtain the deserved credits when they honestly accomplish tasks. Therefore, a secure and fair incentive scheme for cooperatively packet downloading-and-forwarding is desirable, which can also satisfy the requirements of the delay and data rate.

In this paper, we propose a secure incentive scheme for reliable cooperative downloading in highway VANETs, named SIRC, to stimulate vehicle users to help others securely download-and-forward packets. Specifically, SIRC can be divided into two phases: cooperative downloading and cooperative forwarding phase. During the cooperative downloading phase, a client vehicle requests file downloading with a virtual check [12], which is distributed to other vehicles. Motivated by virtual checks, some of vehicles, named proxy vehicles, are willing to help the client vehicle. When a proxy vehicle honestly downloads the packet, it obtains the digital signature of the virtual check as a proof of the successful downloading of the packet. With this digital signature, the proxy vehicle can only obtain part of the check. When the client vehicle receives the whole packet, it signs the check such that the proxy vehicle can obtain all credits. During the cooperative forwarding phase, a profit-sharing model associated with aggregating Camenisch-Lysyanskaya (CL) signature can resist various attacks and reduce the authentication overhead. To summarize, the main contributions of this paper are three fold.

- Firstly, a novel incentive mechanism is proposed to stimulate the packet downloading, which utilizes "virtual checks" associated with the designated verifier signature to ensure fair and secure cooperation and eliminate the demands of accurate knowledge about how many credits to pay. Particularly, to minimize the payment risk of the client vehicle, we design a partial prepayment strategy, i.e., the vehicles involved in downloading packets can only obtain part of the check before the client vehicle confirms the packet reception.
- Secondly, a reputation system is developed to encourage cooperation and punish the malicious vehicles. With the reputation system, the enhanced SIRC is proposed to stimulate the packet forwarding and achieve reliability. Specifically, a downloaded packet can be forwarded through multiple copies. Meanwhile, to ensure fairness, only the first one of these copies arrives at the client vehicle, and the corresponding vehicles involved in forwarding the packet can obtain credit from the proxy vehicles. For other vehicles forwarding the packets successfully, they still can obtain the reputation values.
- Thirdly, we utilize the aggregating CL-signature to guarantee the security of the proposed incentive mechanism. Security analysis show that the SIRC can resist various attacks, including injection/removing attack, free riding attack, submission refusal attack. In addition, SIRC can be equipped with the single pruning search (SPS) or paired single pruning search (PSPS) method to detect and weaken denial of service (DoS) attacks.

The remainder of this paper is organized as follows. We first review the related work in Section II. In Section III, we formalize the network model, define the security requirement, and identify the design goals. In Section IV, we present our SIRC in detail, followed by its security analysis and performance evaluation in Sections V and VI, respectively. Finally, we draw our conclusions in Section VII.

II. Related Work

Incentive schemes for cooperation are extensively studied in multihop cellular network (MCNs) [13], delay tolerant networks (DTNs) [14].

textcolorblueMahmoud and Shen [15] propose a fair, efficient, and secure cooperation incentive mechanism, FESCIM, to stimulate the node cooperation. In scheme [16], Mahmoud *et al*. propose a secure payment scheme RACE using the concept of *Evidence* to secure the payment and requires applying cryptographic operations in clearing the payment only in case of cheating. However, they assume that the clocks of the nodes are synchronized, and their protocol is used with source routing protocol, which establishes end-to-end routes before transmitting data. These assumptions are not suitable for the dynamic networks. Zhu *et al*. [17] propose an incentive scheme, SMART, in a generalized multicopy data-forwarding architecture for DTN. Based on the profit-sharing model, SMART introduces the layered coin to provide the secure payment against a wide range of cheating actions. By utilizing the layered coin architecture, Lu *et al*. [18] further propose an incentive scheme Pi focusing on the fairness issue in the the single-copy case. In their scheme, to achieve fairness, the intermediate nodes can earn credits for forwarding packets and gain reputation for forwarding the undelivered packets.

To improve packet-delivery ratio, reduce data packet delay and overhead, many protocols have been proposed to investigate efficient data delivery issues in vehicular intermittently connected networks, such as [19]–[22]. However, these protocols do not consider whether intermediate nodes are willing to cooperate, and the corresponding incentive and security problems. Particularly, for cooperative download applications, several routing metric has been proposed, including [23]–[26]. For the case that multiple vehicles are requesting the same contents, Hao *et al*. [27] propose a secure cooperative data downloading framework for paid services. In their framework, the vehicles download data when they pass by an RSU and then share the data after they travel out of the RSU's coverage. However, they do not consider the incentive mechanism since all vehicles in their framework are self-interest-driven.

Most of existing secure incentive schemes only involve the cooperative packets forwarding without the consideration of cooperative downloading scenarios. Moreover, compared with the existing application scenarios, e.g., vehicular DTNs in the urban area, the cooperative downloading in highway VANETs has some unique characteristics. For example, in highway VANETs, the vehicles may exit the highway. If other vehicles do not forward packets as quickly as possible,

TABLE I
COMPARISON OF SIRC WITH SEVERAL EXISTING SCHEMES

	Scheme [15]	Scheme [16]	Scheme [17]	Scheme [18]	Scheme [27]	Our Scheme
AS	MCN	MCN	DTN	DTN	VANET	VANET
AT	Packet Forwarding	Packet Forwarding	Packet Forwarding	Packet Forwarding	File Sharing	Downloading Assistance
RS	Pre-	Pre-	Temporary	Temporary	N/A	Temporary
SSD	No	No	No	No	Yes	Yes
SSF	Yes	Yes	Yes	Yes	N/A	Yes
CT	Hybrid	Hybrid	Asymmetric	Asymmetric	Asymmetric	Hybrid
AA	No	No	Yes	Yes	N/A	Yes
PP	Weak	Weak	Common	Common	Common	Strong

AS: application scenario; DG: application type; RS: routing establishment; SSD: support of secure downloading; SSF: support of secure forwarding; CT: cryptographic technique; AA: adoption of aggregate authentication for reducing the communication overhead; PP: privacy preservation

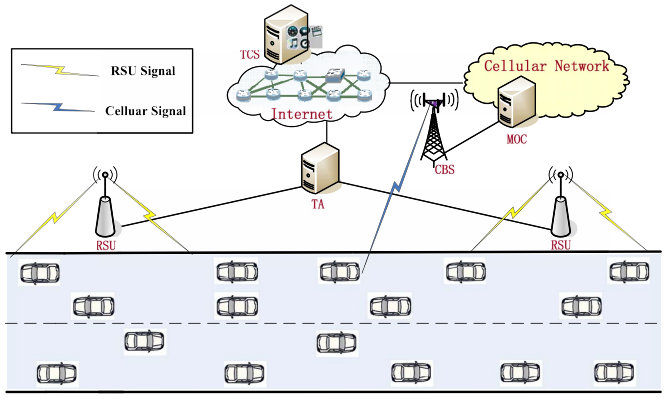


Fig. 1. Network Model.

the packets cannot be delivered to the client vehicle. Therefore, this paper aims to propose a secure incentive scheme for reliable cooperative downloading in highway VANETs. An overall comparison of SIRC with several existing schemes is given in Table I.

III. MODEL AND DESIGN GOALS

In this section, we formalize the network model, define the security requirements and identify the design goals.

A. Network Model

Our network model mainly consists of road side infrastructure (RSU), cellular base station (CBS), vehicles, mobile operator center (MOC), trusted authority (TA), and trusted content server (TCS), as shown in Fig. 1.

- An RSU, e.g., IEEE 802.11n AP, is connected to the Internet backbone, which can provide the Internet services to vehicles driving through the coverage of RSU.
- A CBS, e.g., LTE HeNB, is regulated by a mobile operator, and can also provide wireless access service for vehicles through 4G-LTE cellular network.
- MOC is regulated by the mobile operator, and can provide authentication and security-related services.
- TA that is connected to RSUs can provide authentication and security-related services. It is also a virtual bank, and performs trusted fair credit clearance for assistance vehicles.
- TCS is a trusted authority, which provides downloading services to each authorized vehicle.

To guarantee connectivity, OBUs are installed on the running vehicles, which can communicate with each other over wireless channel [28], [29] for transmitting data, and with RSUs for accessing the Internet. In addition, the built-in cellular module [30] can be utilized to connect the vehicles to the Internet through the CBS. Meanwhile, device to device (D2D) technique can be adopted to achieve reliability of packet forwarding [31].

In the network model, the vehicles can be divided into three categories: client vehicle, proxy vehicle and assistance vehicle. The vehicles that want to download a file on the road can be named as client vehicle. As a proxy vehicle, its main task is to help the client vehicle download a packet on the road. Those vehicles that help the client vehicle forward a packet on the road can be considered as assistance vehicle. Obviously, all vehicles on the road can play different roles.

B. Security Requirements

To guarantee security of SIRC, the corresponding security techniques should be applied. In our security model, all the proxy and assistance vehicles are selfish and curious. Besides, there exists an adversary $\mathcal{A}$ residing in the network, it can eavesdrop, modify or replay the authentication messages. The adversary $\mathcal{A}$ could launch some active attacks to frustrate the procedures of authentication. Therefore, the following security services should be provided:

- *Authentication*: To resist adversary $\mathcal{A}$ and ensure the packet integrity, the forwarded packets should be authenticated hop by hop.
- *Privacy Preservation*: To preserve content privacy, the downloaded packets for client vehicle must be encrypted and cannot be transmitted in plain text. To preserve transaction privacy, a transaction (i.e., a payment of the client vehicle for the proxy vehicle) cannot be verified except for the TA.

In addition, there are several attacks existing in the cooperative packet forwarding, which have been studied by [17] and [18], e.g., layer injection attack, free riding attack, layer removing attack and submission refusal attack. The proposed SIRC scheme must resist or alleviate these similar attacks. Furthermore, the following attacks should also be considered:

• *Black/Gray Hole Attack*: The adversary $\mathcal{A}$ may accept the forwarding task, and actually drop packets later, which is called black hole attack [32]. It obviously is one kind of DoS attacks and can largely degrade the performance of the whole networks. Grey hole attack is a variant of black hole attack, where the adversary $\mathcal{A}$ selectively forwards some packets but not all packets.

• *Denial of Service Attack*: We consider two types of DoS attacks. One is caused by black/gray hole attack, which results in maliciously dropping packets; the other one is caused by invalid signatures in batched signatures, which makes the batch verification fail.

C. Design Goals

This paper focuses on investigating the security and incentive issues and thus its main objective is that all the packets can be reliably transmitted to the client vehicle by using the proposed incentive mechanism without violating the interests of legitimate vehicles. Therefore, similar to previous schemes, e.g., [17], [18], we just consider the process of downloading one file. That is, there is only one client vehicle in the network. Meanwhile, proxy vehicles and assistance vehicles need to strictly carry out their respective tasks despite they can play different roles in other downloading processes.

The proposed SIRC should achieve the following four goals.

1) *Security*. Security is the primary objective in this paper. Without security guarantee, the whole incentive mechanism cannot work properly, resulting in fairness undermining and reliability reduction. Therefore, SIRC should provide authentication and privacy preservation, and resist a wide range of attacks, e.g., injection/removing attack, free riding attack, submission refusal attack, denial of service (DoS) attacks.

2) *Reliability*. Reliability is another important objective in this paper. To achieve reliable cooperative downloading, as many as possible downloaded packets should be delivered to the client vehicle. Only when receiving enough downloaded packets, the client vehicle can recover the file content successfully to achieve reliable downloading.

3) *Fairness*. On one hand, the vehicles involved in helping download-and-forward the packets should obtain the deserved credits when they honestly accomplish tasks without any repudiation. On the other hand, the selfish or malicious vehicles cannot take some cheating actions and cause economic losses to other honest vehicles.

4) *Efficiency*. SIRC should efficiently work without introducing unnecessary cryptographic communication and computation overhead. In addition, SIRC must achieve the high download success rate and low average download delay.

IV. The Proposed SIRC Scheme

In this section, we present the proposed SIRC. The definition of notations in the scheme is presented in Table II.

A. Overview

A client vehicle equipping with an OBU or a built-in cellular module is willing to download a file from the Internet.[1]

[1]To offload the cellular traffic, the vehicles can download the large file from the RSUs, and exchange other data with the cellular networks.

TABLE II
Definition of Notations in the Scheme

Notation	Definition
ID_x	the identity of x
K_{x-y}	the shared secret key between x and y
MAC	the message authentication code
f	the generation function of MAC
H	the secure cryptographic hash function, $H : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$
H_1	the secure cryptographic hash function, $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$
$E_x()$	the symmetrical encryption by using x
$Sig_x()$	the signature of x
TS_x	the timestamp generated by x

Firstly, the client vehicle accesses the TCS by connecting to the CBS, browses and selects the contents stored in the TCS. Secondly, it sends the downloading request to the TCS. If the volume of the file exceeds maximum downloading file size per drive-thru by the vehicle, the TCS divides the file into N chunks based on the evaluated download throughput of individual vehicle, and informs the client vehicle that a cooptative downloading is needed. Afterwards, the client vehicle loads a virtual check in the downloading request message, and distributes these virtual checks to the vehicles driving at the same direction. Then, the client vehicle waits and selects a number of the responded vehicles as proxy vehicles. Note that, to complete downloading, the number of selected proxy vehicles should be more than N. Both the client vehicle and proxy vehicles form a temporary group. Thirdly, when these vehicles move within the coverage of an RSU, they can download the non-overlapping parts of the file from the Internet through the RSU, respectively. Finally, the client vehicle collects all fragments of the file from the group members when they are outside the RSU's coverage.

The SIRC consists mainly of three phases: *proxy vehicle selection phase* (Fig. 2 (a)), *cooperative downloading phase* (Fig. 2 (b)), and *cooperative forwarding phase* (Fig. 2 (c)). In the first two phases, the client vehicle selects the group members from the neighboring vehicles, and allocates the download tasks to them based on their locations and mobility features [11]. The number of group members thus depends on the target data volume to download and mobility of vehicles. In the third phase, the downloaded packets for the client vehicle need to be forwarded by assistance vehicles.

B. Fairness Model

To motivate vehicle users to download the file through the RSU, the mobile operator applies some incentives to ensure vehicle users to obtain reasonable profit $\mathcal{P}$ [6]. To further stimulate the proxy vehicles and assistance vehicles to help download and forward packets, the following hybrid incentive mechanism are adopted.

1) Cooperative Downland Phase: To stimulate the proxy vehicles to help download packets, SIRC utilizes "virtual checks" to eliminate the demands of accurate knowledge about how many credits the client vehicle should pay for proxy vehicles. The client vehicle just needs to load a virtual check ($\mathcal{VC}$)

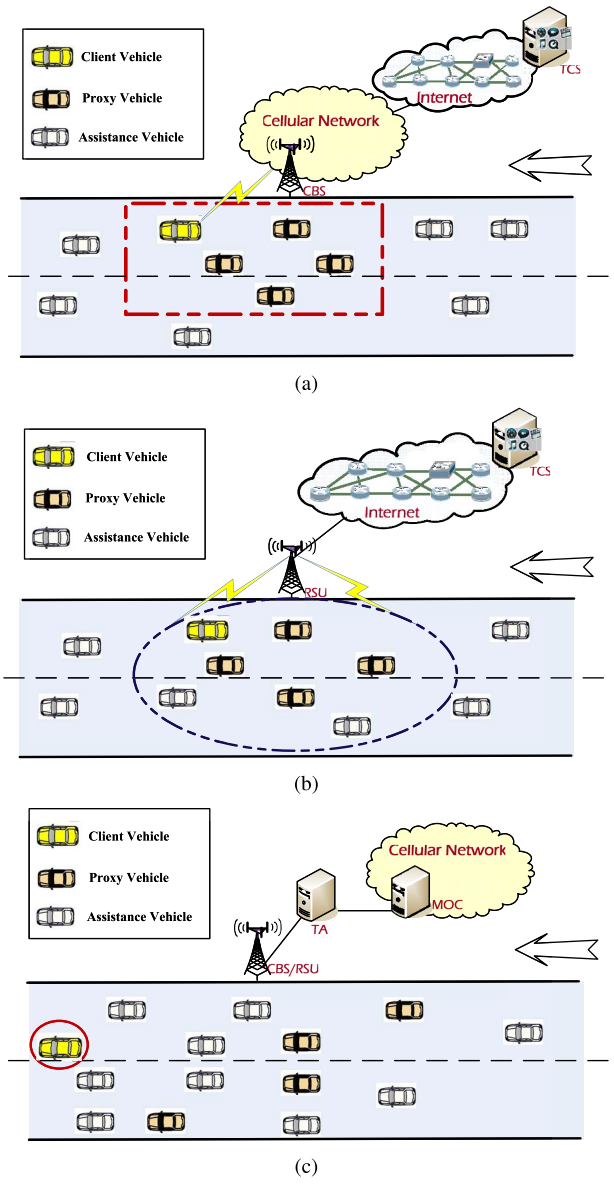


Fig. 2. A cooperative packet downloading and delivery scenario for vehicles. (a) Proxy vehicle selection phase. (b) Cooperative downloading phase. (c) Cooperative forwarding phase.

in the downloading request message, and distributes these virtual checks to the vehicles around it. When a vehicle accepts the request, it becomes a proxy vehicle. Meanwhile, to reduce the payment risk of the client vehicle, we use "partial prepayment" strategy for proxy vehicles. When the proxy vehicle honestly downloads the packet from the TCS, the TCS digitally signs the $\mathcal{VC}$. If the $\mathcal{VC}$ is only signed by the TCS, the proxy vehicle only obtains part of the check, e.g., 50%. We define this ratio as α, where $0 \leq \alpha \leq 1$. When the client vehicle receives the packet, it also signs the $\mathcal{VC}$. Only when both the TCS and the client vehicle have signed the $\mathcal{VC}$, the proxy vehicle can obtain all credits. Obviously, α would influence the cooperation probability of proxy vehicles (P_{pv}). When α varies from 0 to 0.5, the proxy vehicle prefers to cooperate for obtaining the remaining credits, thus P_{pv} increases; but when α exceeds 0.5, the proxy vehicle may weigh the credits it has obtained and the the price it should pay, which would reduce P_{pv}.

2) Reputation System: There exists a situation, i.e., even α is small, the proxy vehicle still might download but not deliver the packet, and there would be the likelihood of a loss for the client vehicle. Therefore, a reputation system needs to be established to punish the selfish proxy vehicles. Apart from the situation mentioned above, we mainly consider two cases that the packet cannot be delivered to the client vehicle: 1) the normal packet loss; 2) the malicious packet dropping by the assistance vehicles. To guarantee fairness, we design a reputation system: If the client vehicle finally do not receive the packet, it reports to the TCS and give a bad review to the proxy vehicle. The TCS calculates the reputation rating according to the bad reviews. Upon the bad reviews accumulate at a certain level, the reputation rating of a vehicle will be reduced and till it is added to the blacklist. If the vehicle in the blacklist, it will not be provided any services until it restores the higher reputation rating.

A threshold value TH_R is set, and when the bad reviews of a vehicle exceed TH_R in one day, the reputation value is calculated once; otherwise, remaining the reputation value unchanged. Let REP_t^- be the vehicle's reputation value at time T, and the reputation value REP_t^- at time T is

$$REP_t{}^- = e^{-\lambda \Delta T} \cdot REP_{t-1}{}^- - Num_{bv}, \tag{1}$$

where ΔT is the time interval between t-1 and t, λ ($\lambda > 1$) is the rate at which the reputation value would decrease, and Num_{bv} is the number of the bad reviews in a day.

3) Cooperative Forwarding Phase: To stimulate assistance vehicles to help forward packets, we propose a profit-sharing model, in which the assistance vehicles involved in a successful packet delivery would be paid with a dividend of the total credit provided by the proxy vehicle. We assume that the total number of assistance vehicles along the successful delivery paths is M, and the proxy vehicle is going to reward these M assistance vehicles with $\mathcal{R}$[2] credits. Therefore, each assistance vehicle receives $\mathcal{R}/M$ credits. Note that, the presence of selfish vehicles would be against the goal of cooperatively delivering a packet from the proxy vehicle to client vehicle. According to [18], the cooperation probability of a selfish vehicle can be

$$P_c = \beta P_s + 1 - \beta, \tag{2}$$

where $0 \leq \beta \leq 1$ is the selfish factor, $P_s < 1$ is the cooperation probability under selfish condition, the smaller the selfish factor β is, the better the cooperation can be completed.

C. Secure Incentive

In this section, to clearly illustrate the scheme, we first consider a single-copy packet forwarding case, i.e., for each packet, only one copy is initially spread by the proxy vehicle. Then this copy is relayed from one assistance vehicle to another until its reaching the client vehicle. Four phases should be performed: system initialization, cooperative file

[2]Obviously, the following relations should hold: $\mathcal{P} > \mathcal{VC} > \mathcal{R}$.

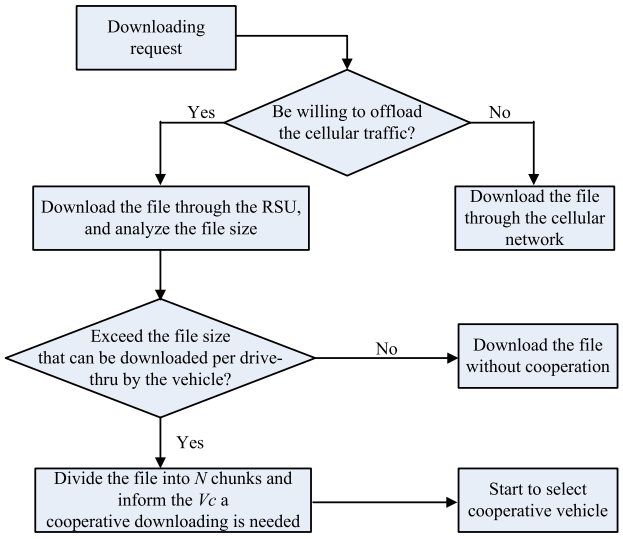


Fig. 3. Selection of the downloading mode.

downloading, cooperative packet forwarding, and rewarding and content recovering.

1) System Initialization: The following works should be completed:

• Firstly, all vehicles who want to download the contents from the TCS must register with the TCS and be authorized by the TCS, then the TCS shares a symmetric key K_{T-V_i} with the authorized vehicles.

• Before joining the VANETs, each vehicle should register itself to the TA and obtain its vehicular credit account (VCA). Later, when a vehicle has an available fast connection to the TA, it can report to the TA for credit clearance. The following parameters are initially shared between each vehicle and the TA [33]: (q, g, H_1), where q is a prime factor of p-1, $g \in \mathbb{Z}_p^*$ is a generator of order q. Both vehicles and the TA choose their secret keys $x_i \in \mathbb{Z}_q$ and publish the corresponding public keys $y_i = g^{x_i} \ mod \ p$.

• Given the security parameters κ, each vehicle first generates $(p, g, \mathbb{G}, \mathbb{G}_T, e)$ by running $\mathcal{G}en(\kappa)$, and then chooses a random element $R \in \mathbb{G}$. The vehicle publishes the system parameters as

$$SP = (p, g, \mathbb{G}, \mathbb{G}_T, e, R) \tag{3}$$

Taking the public parameters SP as input, the vehicle selects a random exponent $\alpha \in Z_p^*$, and calculates $PK = g^\alpha$ as its public key, and keeps the private key α secretly [34].

2) Cooperative File Downloading: When the client vehicle (V_c) is traveling on the road, and the users are willing to download a file from the Internet, V_c sends downloading request to the TCS through the CBS.[3] As shown in Fig. 3, upon the TCS receives the downloading request, it performs the corresponding process to choose the way to download the file. When V_c is willing to download the file by using the RSU, the TCS checks the volume of the file. If the volume of the file exceeds file size that can be downloaded per drive-thru by the vehicle, the TCS divides the file into N chunks based on the evaluated download throughput of individual vehicle, and informs V_c that a cooperative downloading is needed. After that, V_c selects a number of responded vehicles driving at the same direction as proxy vehicles (V_ps), and allocates the download tasks to them based on their locations and mobility features. Consequently, these vehicles form a group provisionally, and all vehicles in the group download the non-overlapping parts of the file from the Internet when they drive within the coverage of the RSU. Concretely, the whole process should occur in two steps:

• *Step-1: Downloading task allocation and authorization.*

- V_c broadcasts the download assistance request messages to those vehicles driving at the same direction, and waits for the responses from them;
- V_c selects $N+i$[4] vehicles from responsive vehicles as its group members, i.e., proxy vehicle (V_p). To stimulate these V_ps to help V_c download the file, V_c generates a virtual check $\mathcal{VC}$;
- To protect personal file privacy, V_c encrypts the name of downloading task (NDT) by using the symmetric key K_{T-V_c} as $EN = E_{K_{T-V_c}}(NDT)$
- V_c generates the message authentication code $MAC_{V_c} = f_{K_{T-V_c}}(\mathcal{VC}||EN||ID_{V_c}||ID_{V_p}||TS_{V_c})$.

After that, V_c sends the message $(ID_{V_c}||MAC_{V_c}||EN||TS_{V_c}||\mathcal{VC})$ to each V_p.

• *Step-2: File downloading.*

The file can be divided into N fragments, denoted as $frag_i, i \in (1, 2..., N)$, which can be downloaded by N vehicles. When the vehicles in the group move into the RSU's coverage successively, each vehicle runs the Algorithm 1. After that, the following procedures are performed:

- The TCS first sends $(ID_{TCS}||C_i||MAC_{T-V_{p_i}}||TS_{TCS})$ to the ith proxy vehicle (V_{p_i}).
- By using $K_{T-V_{p_i}}$, V_{p_i} computes

$$MAC'_{T-V_{p_i}} = f_{K_{T-V_{p_i}}}(C_i||ID_{TCS}||ID_{V_{pi}}||TS_{TCS}), \tag{4}$$

  and verifies if $MAC'_{T-V_{p_i}}$ equals $MAC_{T-V_{p_i}}$. If the verification is successful, V_{pi} sends back acknowledgement (ACK) to the TCS.
- Once receiving ACK, the TCS sends σ_{TCS} to V_{p_i}. The latter keeps σ_{TCS} and $\mathcal{VC}$ for future use.

3) Cooperative Packet Forwarding: When all encrypted fragments of the file are downloaded by vehicles in the group, and all vehicles drive away from the RSU. The proxy vehicles in the group start to deliver N-1 encrypted fragments $(C_1, C_2, \ldots C_{N-1})$ to the client vehicle. Without loss of generality, we provide the detailed procedures of packet forwarding performed by proxy vehicle V_{p_1}. As shown in Fig. 4, firstly, V_{p_1} generates $M_0 = H(C_1||\sigma_{TCS}||ID_{V_{p_1}}||TS_{V_{p_i}})$ and signs M_0 by

[3]The V_c has been authenticated by the cellular network, and a secure channel between V_c and the cellular network has been established.

[4]The selection of i is flexible because of the introduce of $\mathcal{VC}$. The V_c can choose a reasonable i based on the evaluated download throughput of individual vehicle. The greater i is, the higher the download success is, accordingly, the communication overhead becomes larger.

Algorithm 1: The Fragment of the File Downloading

Data: When moving into the RSU's coverage, each proxy vehicle V_{p_i} sends downloading request containing its ID and $(ID_{V_c}||MAC_{V_c}||EN||TS_{V_c}||\mathcal{VC})$ to the TCS. The TCS verifies the validity of MAC_{V_c} and decrypts the EN by using K_{T-V_c}, and retrieves the file that has been preprocessed according to the NDT.

begin
  if *client vehicle* **then**
    TCS chooses one fragment of the file, e.g., $frag_j$, encrypts $frag_j$ using K_{T-V_c}, i.e., $C_j = E_{K_{T-V_c}}(frag_j)$, and sends C_j to the client vehicle directly
  else
    if $i < N$ **then**
      for *each* V_{p_i} **do**
        TCS encrypts $frag_i$ using K_{T-V_c}, i.e., $C_i = E_{K_{T-V_c}}(frag_i)$;
        TCS generates the message authentication code $MAC_{T-V_{p_i}} =$ $f_{K_{T-V_{p_i}}}(C_i||ID_{TCS}||ID_{V_{pi}}||TS_{TCS})$, where TS_{TCS} is the current timestamp. Upon C_i has been downloaded, TCS makes use of a standard signature technique to signs the VC as follows: $\sigma_{TCS} = Sig_{TCS}(H(VC)||ID_{TCS}||ID_{V_{pi}}||TS_{TCS})$
      end
    else
      Stop downloading and send *downloading completed* message
    end
  end
end

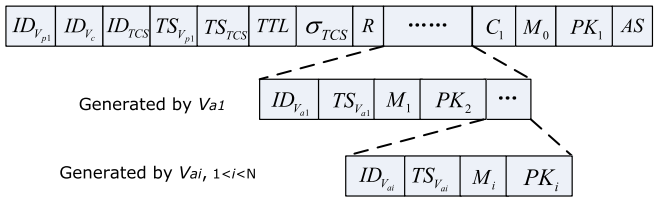


Fig. 4. The format of the V_{p_1}.

executing the Algorithm 2. Furthermore, V_{p_1} having C_1 generates the packet as: $P_{V_{p_1}} = (ID_{V_{p_1}}||ID_{V_c}||ID_{TCS}||TS_{V_{p_i}}||TS_{TCS}||TTL||\sigma_{TCS}||\mathcal{R}||.....||C_1||M_0||PK_1||AS)$.

Where *TS* refers to the packet creation timestamp by each entity, *TTL* represents the time-to-live that signifies the lifetime of the packet, $\mathcal{R}$ is the rewarding provided by V_{p_1}, and *AS* stands for the result of the aggregate signature.

Then, V_{p_1} carrying $P_{V_{p_1}}$ keeps driving on the road till it meets the next vehicle. If that vehicle is V_c, V_{p_1} sends $P_{V_{p_1}}$ to V_c directly; otherwise, the packet needs to be forwarded by the assistance vehicles, and thus the corresponding routing

Algorithm 2: Generation of the AS

input : an aggregate-so-far $AS' = (\sigma_1', \sigma_2', \sigma_3')$ on message $M' = (M_0, M_1, M_2, \ldots, M_{i-1})$ under public keys $\mathbf{PK}' = PK_{i-1}, PK_{i-2}, ...PK_1$, the ith assistance vehicle's private key α_i and public keys PK_i

output: AS or $Halt$

for *the* i*th assistance vehicle,* V_{ai}*, with its private key* α_i **do**
  invoke Algorithm 3 to check AS'
  for $i \leftarrow 2$ **to** *N-1* **do**
    if *the public key* PK_i *of* α_i *does already exist in* $\mathbf{PK}'$ && AS' *is valid* **then**
      generate message $M_i = H(C_1||\sigma_{TCS}||ID_{V_{a_i}}||TS_{a_i})$, and then select a random exponent $\gamma_i \in \mathbb{Z}_p^*$, and compute the aggregate signature as $AS = (\sigma_1, \sigma_2, \sigma_3)$, where

$$\begin{cases} \sigma_1 = (\sigma_1')^{\gamma_i} \\ \sigma_2 = (\sigma_2')^{\gamma_i} \\ \sigma_3 = (\sigma_3' \cdot (\sigma_1')^{\alpha_i} \cdot (\sigma_2')^{\alpha M_i})^{\gamma_i} \end{cases}$$

      return AS
    else
      Halt
    end
  end
end

algorithm should be applied. In other words, SIRC can work with most of the existing routing algorithms [23], [35]. The following steps should be performed:

- *Step-1.* As shown in Fig. 2, the packet is transmitted from the vehicle in the right-hand side to the vehicle in the left-hand side. At the beginning, $P_{V_{p_1}}$ is transmitted from the proxy vehicle to the first assistance vehicle V_{a1}.
- *Step-2.* Then, for two assistance vehicles (designate the left-hand side one as V_{a_i}, and the right-hand side one as $V_{a_{i-1}}$), when V_{a_i} receives the packet $packet_{i-1}$ sent from $V_{a_{i-1}}$, it first checks the $\mathcal{R}$ and decides if it is willing to help to forward this packet.
- *Step-3.* Once V_{a_i} accepts this request, it verifies the validity of $packet_{i-1}$ by invoking the Algorithm 3. If the verification passes, V_{a_i} generates $M_i = H(C_1||\sigma_{TCS}||ID_{V_{a_i}}||TS_{V_{a_i}})$, and adds its own authentication information $(ID_{V_{a_i}}||TS_{a_i}||M_i||PK_i)$ to the corresponding area in $P_{V_{p_1}}$ (as shown in Fig. 3). V_{a_i} also computes new AS by executing Algorithm 2 to update the previous AS'. Then, V_{a_i} sends the updated packet $packet_i$ to the next vehicle $V_{a_{i+1}}$.

4) Rewarding and Content Recovering: Upon receiving final packet sent from $V_{a_{N-1}}$, the client vehicle V_c first verifies the validity of AS by invoking the Algorithm 3. Then, V_c verifies the validity of σ_{TCS}. If the verification passes, V_c confirms that V_{p_1} has downloaded the corresponding fragment

Algorithm 3: Verification of the AS

input : AS and all i-1 assistance vehicle's **PK** $= (PK_{i-1}, PK_{i-2}, ...Pub_1)$ before V_{a_i}
output: 0, 1 or $Halt$

for *the* i*th vehicle* **do**
  if *any public key does not appear twice in* **PK then**
    verify that

$$\begin{cases} e(\sigma_1, R) \stackrel{?}{=} e(\sigma_2, g) \\ e(\sigma_3, g) \stackrel{?}{=} e(\sigma_1, \prod_{j=1}^{i-1} PK_j) \cdot (\sigma_2, \prod_{j=1}^{i-1} PK_j^{M_j}) \end{cases}$$

    if *this equation holds* **then**
      return 1
    else
      return 0
    end
  else
    return *Halt*
  end
end

of the file from the TCS; otherwise it can refuse to bill the $\mathcal{VC}$ for V_{p_1}.

After that, V_c generates $M_N = H(C_1||\sigma_{TCS}||ID_{V_c}||TS_{V_c})$, AS and $packet_N$ by executing Algorithm 2. Meanwhile, it signs a special signature on $M_{V_c} = (ID_{V_c}||ID_{V_{p_1}}||ID_{TA}||H(\mathcal{VC})||TS_{V_c})$ as follows: V_c selects two random numbers $k \in Z_q$ and $t \in \mathbb{Z}_q^*$, and computes

$$\begin{cases} c = y_{TA}^k \mod p, \\ r = H_1(M_{V_c}||c), \\ s = kt^{-1} - rx_{V_c} \mod q. \end{cases} \quad (5)$$

$\sigma_{V_c} = (r, s, t)$ is then the signature of M_{V_c}.

When finishing the works above, V_c sends ($packet_N$, M_{V_c}, σ_{V_c}) back to the last assistance vehicle $V_{a_{N-1}}$. After verifying the validity of $packet_N$, $V_{a_{N-1}}$ can submit ($packet_N$, M_{V_c}, σ_{V_c}) to the TA for clearance in the future.

When the last assistance vehicle $V_{a_{N-1}}$ has available fast connection to the TA, $V_{a_{N-1}}$ reports ($packet_N$, M_{V_c}, σ_{V_c}) to the TA, and then the TA performs the clearance as the following steps:

- For the assistance vehicle,
- *Step-1.* The TA checks the freshness and the validity of $packet_N$. If it is fresh and valid, the TA continues; otherwise terminates the operation.
- *Step-2.* According to the incentive policy in $\mathcal{R}$, the TA stores the merited credits in each assistance vehicle's VCA, and withdraws the corresponding credit values from the proxy vehicles' VCAs.

When other assistance vehicles connect to the TA, they can obtain their credits from their own VCAs.

- When the proxy vehicle V_{p_1} connects to the TA,
- *Step-1.* V_{p_1} submits its own σ_{TCS} and $\mathcal{VC}$ to the TA, and then the TA checks the freshness and the validity of σ_{TCS}. If it is fresh and valid, the TA continues; otherwise terminates the operation.
- *Step-2.* Knowing that σ_{V_c} is originated from V_c, the TA verifies the validity of σ_{V_c} by checking

$$H_1(M_{V_c}||(g^s y_{V_c}^r)^{tx_{TA}} \mod p) \stackrel{?}{=} r. \quad (6)$$

Only when both σ_{TCS} and σ_{V_c} are verified successfully, the proxy vehicle V_{p_1} can obtain all credits.

Meanwhile, the client vehicle performs the following steps to recover the file content:

- *Step-1.* When V_c obtains all encrypted fragments $C_{N-1}...||C_1$ from the packets sent from $V_{a_{N-1}}$,...,V_{a_1}, and then combine its own encrypted fragment with $C_{N-1}||C_{N-1}...||C_1$, i.e., $C_N||C_{N-1}...||C_2||C_1$.
- *Step-2.* V_c decrypts $C_N||C_{N-1}...||C_2||C_1$ successively by using K_{T-V_c} shared between the V_c and the TCS.
- *Step-3.* After decryption, the format of the file fragments is $frag_N||frag_{N-1}...||frag_2||frag_1$, V_c combines these file fragments and recovers file content.

D. Enhanced SIRC for Reliable Packet Delivery

To enhance the reliability of packet delivery, we further propose an enhanced SIRC, which can make packet delivery more reliable by adopting the multi-path forwarding, i.e., sending the multiple copies of one packet by different paths to enhance reliability of the packet delivery.

A reputation-based incentive mechanism is introduced, which can further stimulate those vehicles to help forward packets. Due to adopting multi-path forwarding, one downloaded packet can be forwarding through multiple copies. For assistance vehicles, only the first one of these copies arrives at the client vehicle, the relevant assistance vehicles can obtain the credit from proxy vehicles. Therefore, each vehicle does their utmost to forward the packet as soon as possible. On the other hand, for the other assistance vehicles forwarding the packets successfully, their contributions cannot be ignored, and they can still obtain good reputation values from the mobile operator.

1) Additional Incentive Strategy: To reward those assistance vehicles forwarding successfully but not the first ones, we propose a reputation-based incentive mechanism:

- There exists an MOC in the mobile operator network, and the MOC performs trusted reputation clearance on behalf of the mobile operator for assistance vehicles. Before joining the VANET, each vehicle should register itself to the MOC and obtain its vehicular reputation account (VRA) in the initialization phase.
- The VRA records dynamic reputation value of the corresponding vehicle as follows: let REP_t^+ be the assistance vehicle's reputation value at time T, and the reputation value REP_t^+ at time T is

$$REP_t{}^+ = e^{-\lambda \Delta T} \cdot REP_{t-1}{}^+ + Num_{gv}, \quad (7)$$

where ΔT is the time interval between t-1 and t, λ ($\lambda > 1$) is the rate at which the reputation value would decrease, and Num_{gv} is the number of the good reviews in a day.

• An assistance vehicle V_{a_i} helps forward a copy of the ith packet for the client vehicle, but the copy is not the first one arriving at the client vehicle. Even so, V_{p_i} consumes a certain amount of energy (e.g., gas or electricity), denoted as Eng_i. Therefore, it can obtain the corresponding reward $(REP \cdot Eng_i)$, where REP is a fixed unit reputation value provided by the mobile operator for offloading its traffic.

2) Achieving Reliable Packet Delivery Through Multi-Path Forwarding: When a proxy vehicle, without loss of generality, specified as V_{p_1}, is going to deliver V_{p_1}, it just needs to add the REP to $P_{V_{p_1}}$. When the relevant assistance vehicles finish the packet delivery, based on the REP, the incentive policy, and the amount of energy $(Eng_1, Eng_2, \ldots, Eng_i ...)$ recorded in each assistance vehicle's authentication information, the MOC stores the merited reputation values provided by the mobile operator in each assistance vehicle's VRA. If the copy of one packet is not the first to arrive at the client vehicle, each assistance vehicle which helped forwarding can obtain the reputation value from the MOC according to the reputation value calculation method.

V. Security Analysis

In this section, we discuss the security properties of the proposed SIRC scheme.

A. Authentication

In the SIRC, the authentication can be achieved as follows: 1) In the cooperative file downloading phase, the client vehicle V_c generates MAC_{V_c} to make its message $\mathcal{VC}$ and EN not be modified illegally. Similarly, the TCS generates $MAC_{T-V_{p_i}}$ to make its message C_i not be tampered illegally; 2) In the cooperative packet forwarding phase, SIRC utilizes the sequence aggregate signature technique to achieve the hop-by-hop authentication between all assistance vehicles; 3) In the rewarding and content recovering phase, the client vehicle generate its own signature σ_{V_c} by using the designated verifier signature technique. Only when both σ_{TCS} generated by the TCS and σ_{V_c} are verified successfully, the proxy vehicle can obtain all credits.

B. Privacy Preservation

The privacy preservation can be also preserved in the following two aspects:

• To protect personal profiles privacy, the client vehicle V_c encrypts the name of downloading task (NDT) by using the symmetric key K_{T-V_c}, and the TCS encrypts $frag_i$ using K_{T-V_c};

• To preserve transaction privacy, a transaction (i.e., a payment of the client vehicle for the proxy vehicle) can only be verified by the TA. The designated verifier signature technique can achieve this goal, in which nobody else other than the TA can perform the verification of σ_{V_c}, since the TA's secret key is involved in the verification equation. Hereafter, even if the TA reveals its secret key, it cannot convince another party of the validity of σ_{V_c}. Thus this function can preserve transaction privacy of the V_c, i.e., no one can ascertain if the client vehicle V_c has ultimately completed the deal for downloading a file.

Theorem 1: Even though the TA gives its own secret key to the third party, there is no reason that the third party accepts its signature as a client vehicle's signature.

Proof: The TA could simulate a transcript as follows: The TA randomly selects $s^{'} \in \mathbb{Z}_q$ and $r^{'} \in \mathbb{Z}_q^*$ and computes

$$\begin{cases} c = g^{s^{'}} y_{V_c} \mod p, \\ r = H_1(M_{V_c}||c), \\ l = r^{'} r^{-1} \mod q, \\ s = s^{'} l^{-1} \mod q, \\ t = l x_{TA}^{-1} \mod q. \end{cases} \tag{8}$$

Then $c = (g^s y_{V_c}^r)^{t x_{TA}} \mod p$ and $H_1(M_{V_c}||c) = r$, since

$$\begin{aligned} & (g^s y_{V_c}^r)^{t x_{TA}} \mod p \\ &= (g^s y_{V_c}^r)^l \mod p \\ &= g^{sl} y_{V_c}^{rl} \mod p \\ &= g^{s^{'}} y_{V_c}^{r^{'}} \mod p \\ &= c \end{aligned} \tag{9}$$

and $H_1(M_{V_c}||c) = r$ by definition. Therefore, the TA is capable to generate the same transcripts in an indistinguishable way. Even though the TA gives its own secret key to the third party, there is no reason that the third party accepts its signature as a client vehicle's signature. ■

C. Attack Resistance

We focus on the following attacks according to Section III.

• *Injection/Removing Attack*: Similar to the multilayer credit-based incentive schemes [17], [18], the injection/removing attack could be launched by some selfish vehicles. Because in the packet forwarding phase of the SIRC, a profit-sharing model is provided, in which the assistance vehicles involved in a successful packet delivery would be paid with a dividend of the total credit. In this case, the selfish vehicle could add or remove some authentication information in the corresponding area of the packet $P_{V_{p_i}}$ generated by the proxy vehicle. The structure of $P_{V_{p_i}}$ determines its vulnerability. Therefore, we utilize the sequence aggregate signature technique to achieve the hop-by-hop authentication between all assistance vehicles, the secure $P_{V_{p_i}}$ can be built as Fig. 3. With this technique, each following assistance vehicle can easily detect the injection/removing attack by checking the AS.

• *Free Riding Attack*: The free riding attack can be conducted by two selfish vehicles that want to exchange packets without paying their credits. Assume the assistance vehicle V_{a_i} wants to send $M^{'}$ to $V_{a_{i+2}}$ by piggybacking it with the forwarded $packet_i$, the free riding $M^{'}$ cannot pass the verification since AS can provide integrity protection. Therefore, by checking AS, $V_{a_{i+1}}$ can detect the free riding $M^{'}$ and delete it before forwarding it to $V_{a_{i+2}}$.

• *Submission Refusal Attack and Downloading but Not Delivery*: By adopting multi-path forwarding method, SIRC can reduce the risk of the submission refusal attack, which

has been investigated in [17]. In addition, we consider a special case in the cooperative downloading, i.e., downloading but not delivery. As we mentioned in IV-B, to stimulate the proxy vehicles to help downloading packets, SIRC utilizes virtual checks and the pre-paid part of check to lower the risk of the client vehicle. When the proxy vehicle honestly downloads the corresponding packet from the TCS, the TCS digitally signs the $\mathcal{VC}$, i.e., $\sigma_{TCS} = Sig_{TCS}(H(VC)||ID_{TCS}||ID_{V_{pi}}||TS_{TCS})$. If the $\mathcal{VC}$ is only signed by the TCS, the proxy vehicle only obtains part of the value of the check, e.g., 50%. Only when the client vehicle receives the packet, it signs the $\mathcal{VC}$ and generate the signature σ_{V_c}. After that, the proxy vehicle can obtain all credits. It is obvious that the smaller α is, the smaller the risk of the client vehicle is but the lower the enthusiasm of the proxy vehicle is, and vice versa. In addition, even α is small, the proxy vehicle still might download but not deliver the packet, and there would be the likelihood of a loss for the client vehicle. Therefore, a reputation system has been developed to punish the selfish proxy vehicles.

•*Black/Gray Hole Attack*: Due to the hop-by-hop authentication, the black (grey) attacks launched by the external adversary can be efficiently resisted in the proposed SIRC protocol. However, once the assistance vehicles controlled by the adversary $\mathcal{A}$ launch the black (grey) attacks, because they know the valid key materials, the black (grey) attacks in this case are serious and hard to resist. We can adopt a *witness* to resist this attack. The *witness* is required to submit to the TA by each assistance vehicle. If the client vehicle does not receive a packet, then with the chain tracking policy [36], each next-hop assistance vehicle participating in packet forwarding can be identified by the TA with the *witness* provided by the assistance vehicle, where the destination (e.g., the client vehicle's unique ID) is used to assist the current assistance vehicle to identify the involved next-hop assistance vehicle among many next-hop assistance vehicles. If the current assistance vehicle cannot provide any witness, it becomes suspicious. If the time-to-live of a packet passes, the packet can be dropped. However, this packet dropping event is less than the event caused by the packet dropping due to black (grey) hole attacks. Therefore, with Algorithm 4, the assistance vehicles who launched the black (grey) hole attacks can be identified.

• *DoS Attack*: We have analyzed black/gray hole attack, and thus we focus investigating another DoS attack, i.e., invalid signatures in aggregating CL-signature, which leads to failed verification. Obviously, this is another kind of DoS attacks. Fortunately, we can find efficient solutions from previous works. Inspired by [37], we can utilize the single pruning search (SPS) method or paired single pruning search (PSPS) method to detect attackers, and weaken this attack.

Algorithm 4: Detection of Black/Gray Hole Attack

Data: With the chain tracking, the TA can obtain each assistance vehicle V_{ai}'s packet dropping number, denoted as N_i.

Calculate the mean $\overline{N_i}$ of all assistance vehicles as $\overline{N_i} = \frac{1}{N_{V_{ai}}} \sum_{i=1}^{N_{V_{ai}}} N_i$, where $N_{V_{ai}}$ is the number of assistance vehicles.

Calculate the distance of each N_i to the mean $\overline{N_i}$ as $d_i = |N_i - \overline{N_i}|$

Define the thresholds T_b, T_g for black hole attack and grey hole attack, respectively.

```
for each assistance vehicle V_ai do
    if d_i > T_b then
        V_ai is considered as a black hole attacker.
    else
        if d_i > T_g then V_ai is considered as a gray hole attacker.
        else V_ai is considered as a normal assistance vehicle.
    end
end
```

VI. Performance Evaluation

In this section, we first evaluate the performance of the proposed SIRC scheme in terms of cryptographic computation and communication overhead. Then, we analyze the effect of proposed incentive mechanism. In addition, we further demonstrate the effectiveness and efficiency of the SIRC in stimulating proxy and assistance vehicles with extensive simulations.

A. Computation and Communication Overhead

We evaluate computation and communication overhead used to provide security protection in the cooperative file downloading, cooperative packet forwarding, and rewarding and content recovering phases.

1) Computation Overhead: The SIRC adopts a symmetric cryptosystem rather than using the public cryptosystem. The reason is that: a) the symmetric cryptosystem requires a smaller secret key length at the same level of security; b), the encryption and decryption of the symmetric cryptosystem is much faster than that of the public cryptosystem. Because the OBUs are resource-constrained, symmetric cryptosystem can reduce the computational consumption.

In the cooperative file downloading phase, to protect the personal file privacy, two symmetric encryptions are used, they are $EN = E_{K_{T-V_c}}(NDT)$ and $C_i = E_{K_{T-V_c}}(frag_i)$, respectively. To protect the integrity of the messages, two message authentication codes MAC_{V_c} and $MAC_{T-V_{p_i}}$ are generated. All of MAC computation and symmetric encryptions and decryptions can be considered negligible compared to others, e.g., exponentiation and pairing operations. According to [38], we evaluate the computation overhead on a 3.0 GHz machine with 512 MB-memory, based on the PBC [39] and MIRACL [40] libraries. The experimental results indicate that a single exponentiation operation (T_{exp}) in almost costs 12.4 ms, and the corresponding pairing operation (T_{pair}) costs 20 ms.

In the cooperative packet forwarding phase, to achieve hop-by-hop authentication and protect the integrity of $P_{V_{p_i}}$,

TABLE III
SETTING OF PARAMETERS

Parameters	ID	MAC	$\mathcal{R}$	$\mathcal{VC}$	TS	TTL	σ_{TCS}
Value (bits)	32	64	80	80	32	32	160

the sequence aggregate signature technique is adopted. The aggregate signing algorithm requires one aggregate verification and five exponentiations, and the aggregate verification algorithm requires five pairing operations and x exponentiations where x is the number of vehicles that generate the AS during the cooperative packet forwarding. Therefore, the aggregate signing algorithm needs $(5+x)T_{exp}+5T_{pair}=162+12.4x$ ms, and the aggregate verification algorithm requires $xT_{exp}+5T_{pair}=100+12.4x$ ms. The total computation overhead is $262+24.8x$ ms.

In the rewarding and content recovering phase, the aggregate signing algorithm has been performed once, and the aggregate verification algorithm has been performed three times. Besides, the designated verifier signature technique is adopted to preserve transaction privacy. We only consider the number of modular exponentiations, which are the most time-consuming operations. The generation algorithm needs two exponentiations, and the verification algorithm requires three exponentiations. Therefore, the aggregate signature algorithm costs 311.6 ms, and designated verifier signature algorithm requires $5T_{exp}=62$ ms. The total computation overhead is 373.6 ms.

2) Communication Overhead: Table III is the setting of parameters for evaluating performance.The symmetric encryption algorithm adopted in this paper is Advanced Encryption Standard (AES) with 192 key size.

In the cooperative file downloading phase, we first consider the communication of downloading task allocation and authorization, where the client vehicle generates its message $ID_{V_c}||MAC_{V_c}||EN||TS_{V_c}||\mathcal{VC}$ and deliver this message to each proxy vehicle. Therefore, its size should be

$$S_1 = 32+64+|EN|+80 = 208+|EN|\ bits \quad (10)$$

During file downloading, when moving into the RSU's coverage, each proxy vehicle sends the downloading request containing its ID and message $ID_{V_c}||MAC_{V_c}||EN||TS_{V_c}||\mathcal{VC}$ to the TCS, the size of this message is

$$S_2 = 2\times 32+64+|EN|+|TS|+80 = 240+|EN|\ bits \quad (11)$$

Later, the TCS sends back $ID_{TCS}||C_i||MAC_{T-V_{p_i}}||TS_{TCS}$ and σ_{TCS} to the ith proxy vehicle, its size is

$$S_3 = 32+|C_i|+64+32+160 = 256+|C_i|\ bits \quad (12)$$

In the cooperative packet forwarding phase, the proxy vehicle first generates the packet $P_{V_{p_1}}$. Whereafter each assistance vehicle adds its authentication information to the original packet. Due to adopting the sequence aggregate signature technique, the size of AS never changes, which can reduce the communication overhead significantly. Assume there are M vehicles during the cooperative packet forwarding, if the asymmetric bilinear groups using the 175-bit MNT curve with embedding degree 6 to guarantee 80-bit security level, the size of $packet_N$ is

$$S_4 = 1328+749M+|C_i|\ bits \quad (13)$$

In the rewarding and content recovering phase, when finishing the corresponding works, the client vehicle sends $packet_N$, M_{V_c}, σ_{V_c} back to the last assistance vehicle $V_{a_{N-1}}$. After verifying the validity of $packet_N$, the $V_{a_{N-1}}$ can submit $packet_N$, M_{V_c}, σ_{V_c} to the TA for clearance in the future. The total size of the messages is

$$S_5 = 6394+1498M+2|C_i|\ bits \quad (14)$$

From Equations (10)-(14), i.e., S_1-S_5, the packet size (i.e., control packets are added to ensure the security and support the cooperative downloading credit) only depends on the file size and transmission hops, and will not increase with the number of signature since we have applied the aggregating CL-signature technique, which significantly reduces the whole communication overhead. The communication overhead during the cooperative packet forwarding phase is shown in Fig. 5.

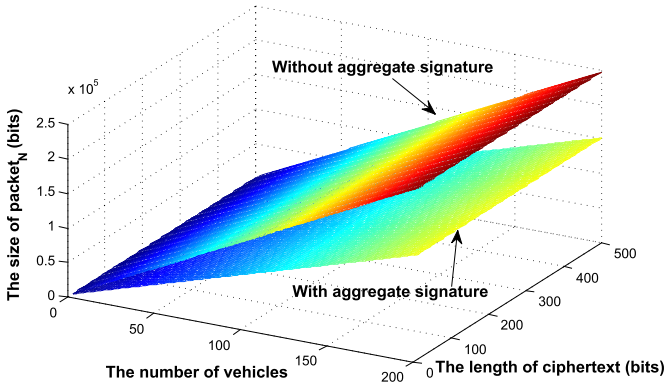


Fig. 5. Communication overhead during the cooperative packet forwarding phase.

B. Analysis of Incentive Mechanism

We analyze several factors that might influence the effect of incentive mechanism.

1) Reputation Rating: According to the IV-B and IV-D, we can obtain the REP_t^- and REP_t^+, respectively. For REP_t^-, we can conclude that: 1) The larger λ is, the quicker the reputation value REP_t^- decreases. 2) Because REP_t^- is calculated only when $Num_{br} > TH_R$, the smaller TH_R is, the calculation of the reputation value is more frequent. Accordingly, the REP_t^- decreases more quickly. 3) The greater Num_{br} is, the REP_t^- also decreases more quickly. We can flexibly develop our reputation rating mechanism by adjusting the TH_R and λ.

For $REP_t{}^+$, the larger λ is, the quicker the reputation value REP_t^+ decreases. Therefore, assistance vehicles must keep and increase their reputation values constantly. We can find that, by adopting our reputation system, a vehicle should try to avoid obtaining too much bad reviews since that would lead him into the blacklist. Conversely, a vehicle can obtain the enough reputation value only by providing a large number

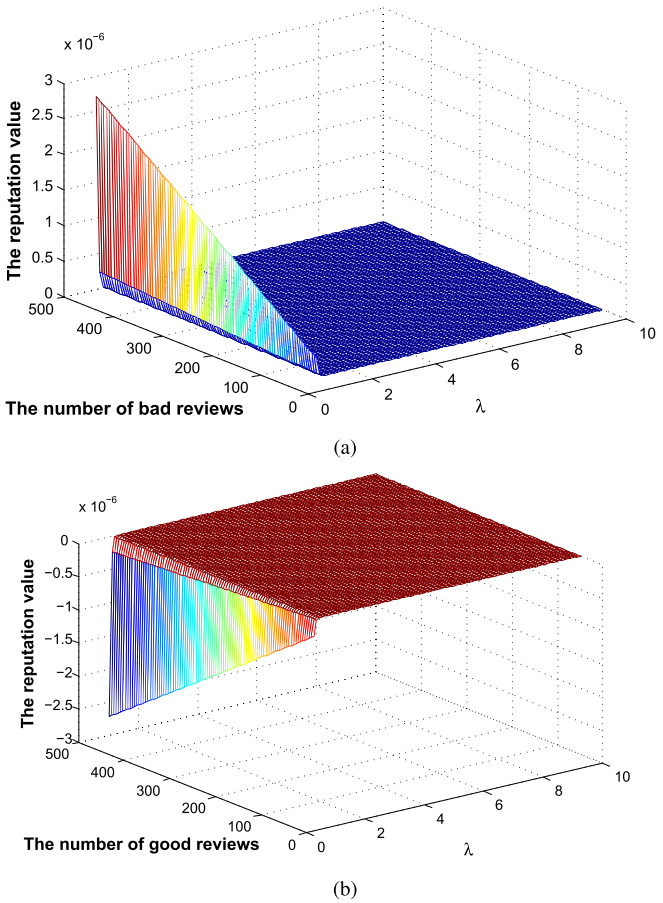


Fig. 6. The changing tendency of the reputation value. (a) REP_t^-. (b) REP_t^+.

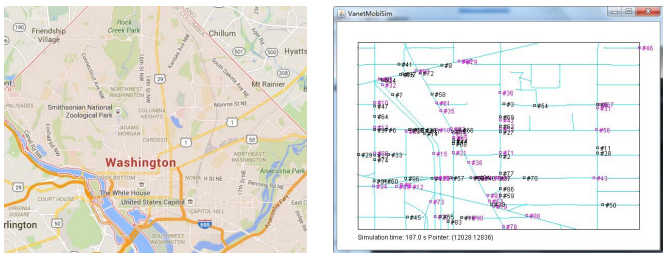
of forwarding services. Hence, our proposed incentive mechanism is effective. The changing tendency of the reputation value is shown in Fig. 6.

2) Single-Copy Forwarding vs. Muti-Copy Forwarding: The number of copies of the packet N_{cp} would influence the download success rate. By sending the multiple copies of one packet by different paths, the reliability of packet delivery can be enhanced. Obviously, when some incentives are provided, the more the number of copies of packet are, the higher the reliability of the packet delivery is; however, because the capacity of the whole network is limited, the excessive copies would degrade the performance of the network. The further evaluation is performed in the following section.

C. Simulation

In this section, we evaluate the performance of the proposed SIRC during the cooperative packet forwarding by using the Vehicular Ad Hoc Networks Mobility Simulator (VanetMobiSim) [41], [42]. The performance metrics used in the evaluation are: i) the success download rate, which is the number of the packets of the downloaded file that are successfully delivered to the client vehicle within a given time period; 2) the average download delay, [5] which is defined as

[5]In this simulation, the average download delay actually equals average forwarding delay since we have assumed that all packets have been downloaded, and the download performance evaluation is out of scope of this paper.



(a) (b)

Fig. 7. Map of the simulation scenario: District of Columbia. (a) Map of District of Columbia. (b) Simulation area under consideration.

the duration between the moment that the first packet is sent out by the proxy vehicle and the time that the final packet is received by the client vehicle. Both the success download rate and average download delay can be used to examine the ability of the proposed SIRC scheme with some incentive strategy to deliver the packets to the client vehicle within a specified period.

1) Simulation Setup: The spatial environment is initialized from the real geographic data source TIGER (Topologically Integrated Geographic Encoding and Referencing) [43], which is created by the United States Census Bureau. The TIGER data of District of Columbia is unitized as the simulation scenario in our paper, as shown in Fig. 7. We specify the multi-lane roads to model highways and therefore generate the multi-lane highway starting from one border and ending on a different border by using the Dijkstra shortest path algorithm. In addition, we simulate all vehicle's motion using the Intelligent Driver Model with Lane Changing (IDM_LC) Model [44].

Because in the drive-thru Internet, a single vehicle can only download around 9 MB file per drive-thru, the different file sizes are needed to be downloaded by different number of proxy vehicles. When each proxy vehicle has downloaded the corresponding packet of the file, it sends out this packet with the incentive when it meets the next vehicle within the efficient communication range. In our simulation, each vehicle is randomly assigned a selfish factor β. If that vehicle is willing to help to forward the packet, it becomes the assistance vehicle. The assistance vehicle performs the same procedure when it meets another vehicle until all packets are successfully delivered to the client vehicle.

The detailed parameter settings are summarized in Table IV. In the following, we run the simulations with different parameter settings, including different number of vehicles, file sizes, selfish factors, incentives and number of copies of one packet. For each case, we run the simulation 100 times, and the average success download rate and average download delay are reported.

2) Simulation Results: The main goal of the SIRC is to provide reliable packet downloading for the client vehicle. Reliable packet downloading indicates eventually, all downloaded packets should be delivered the client vehicle successfully. Because in the drive-thru Internet, a single vehicle can only download around 9 MB file per drive-thru, when the file size is 45 MB, the file should be divided to 45/9=5 packets. Accordingly, 5 proxy vehicles are needed to cooperatively

TABLE IV
SIMULATION SETTINGS

Parameter	Setting
Map bounding	$< westbc >$-77.119759 $< eastbc >$-76.909393 $< northbc >$38.995845 $< southbc >$38.791645
Simulation time	1000 s
TTL	1000 s
Number of vehicles	(50, 100)
File size	(45 MB, 180 MB)
Communication range	300 m
Average data transmission rate	12 Mbps
Velocity of vehicles	90 - 130 km/h
Routing algorithm	POMP
Selfish factor of each vehicle	$\beta \in$[0.2, 0.8]
Incentive (related to P_s)	$P_s \in$ [0, 90%]
Number of copies of one packet	$N_{cp} = [1, 2]$

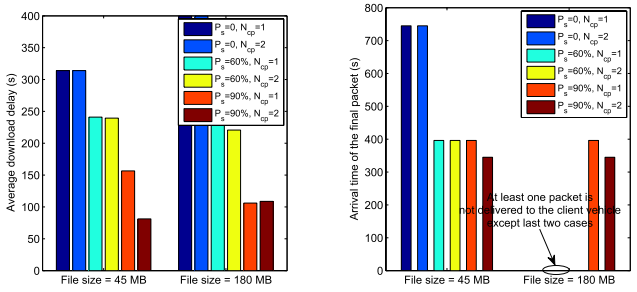


Fig. 8. The download performance for vehicle's ID = 50, when number of vehicles=50. (a) The average download delay. (b) The arrival time of the final packet.

download the file. Similarly, when the file size is 180 MB, the file should be divided to 180/9=20 packets, and 20 proxy vehicles are needed to cooperatively download the file.

An important index to evaluate the performance of SIRC is the average download delay. That is to say, all the packets should not only be delivered to the client vehicle successfully, but also with the minimum delay. In addition, different from other packet delivery scenarios, the more packets are delivered to the client vehicle successfully, and more likely the client vehicle can recover the file content. Therefore, we also analyze the arrival time of the final packet in several cases. To do so, we choose two users, i.e., vehicle's ID = 50 when the number of vehicles is 50, and vehicle's ID = 100 when the number of vehicles is 100. The detailed analysis of these two users on the average download delay and the arrival time of the final packet are given. From Fig. 8 and Fig. 9, we can clearly see that in all situations, when the incentive reaches to 90%, and the number of copies is 2, the average download delay is minimum. We also can observe that except the last two cases, i.e., $P_s = 90\%$ and $N_{cp} = 1$, and $P_s = 90\%$ and $N_{cp} = 2$; in other cases of different number of vehicles and file size, either the arrival time of the final packet is long or the packets are delivered unsuccessfully. Only when $P_s = 90\%$ and $N_{cp} = 2$, the arrival time of the final packet is less than that of other cases.

To further evaluate the download delay, we plot Fig. 10 according to the results by running the simulation 100 times.

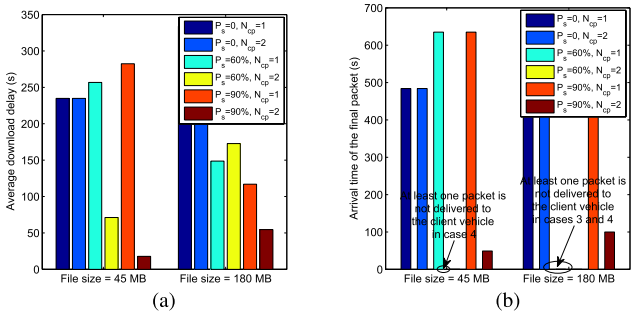


Fig. 9. Download performance for vehicle's ID = 100, when number of vehicles=100. (a) The average download delay. (b) The arrival time of the final packet.

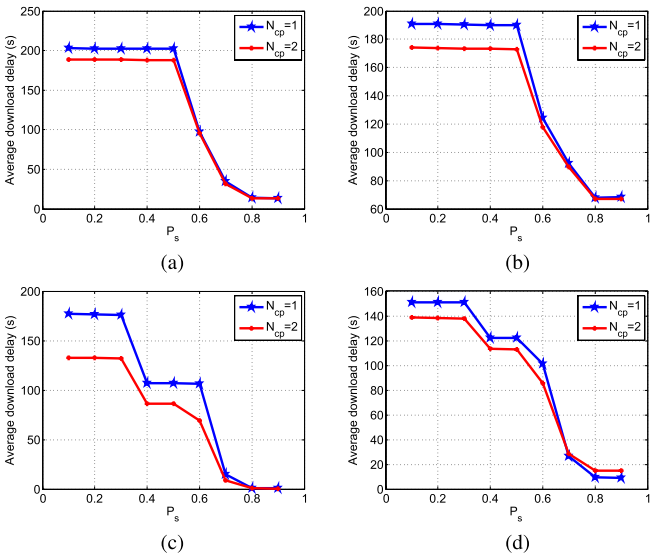


Fig. 10. Average download delay. (a) File size=45 MB, Number of vehicles=50. (b) File size=180 MB, Number of vehicles=50. (c) File size=45 MB, Number of vehicles=100. (d) File size=180 MB, Number of vehicles=100.

Fig. 10 shows the average download delay of SIRC in several different cases. We can observe that the average download delay reduces drastically with the increase of the P_s, which indicates that the high incentive can result in low download delay. Moreover, we can find that the average download delay when N_{cp} equals 2 are smaller than the case that N_{cp} equals 1, especially when the high incentive is applied. Therefore, we can conclude that the proposed SIRC scheme with the high incentive and the multi-copy forwarding is most effective in terms of the download delay.

Similarly, to evaluate the download success rate, we plot Fig. 11 according to the results by running the simulation 100 times. From Fig. 11, we can clearly see that the average download success rate rises significantly with the increase of the P_s, which indicates that the high incentive can result in high download success rate. Furthermore, we can observe that the download success rate when N_{cp} equals 2 are larger than the case that N_{cp} equals 1, especially when the high incentive is applied. Therefore, we can also conclude that the proposed SIRC scheme with the high incentive and the multi-copy forwarding is most effective in terms of the download success rate.

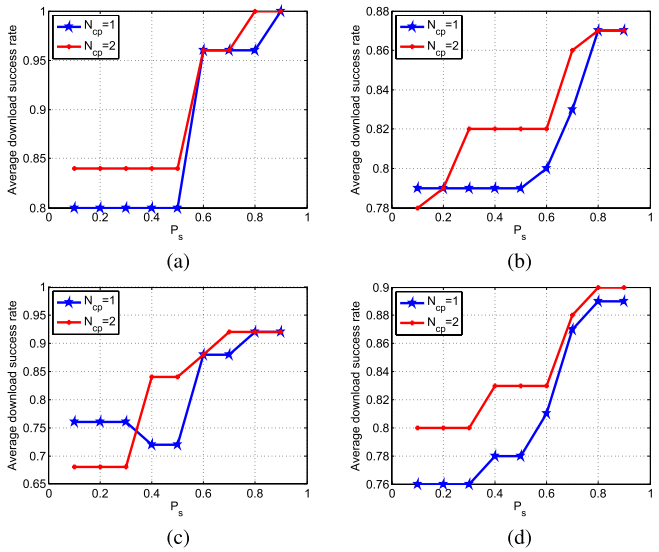


Fig. 11. Average download success rate. (a) File size=45 MB, Number of vehicles=50. (b) File size=180 MB, Number of vehicles=50. (c) File size=45 MB, Number of vehicles=100. (d) File size=180 MB, Number of vehicles=100.

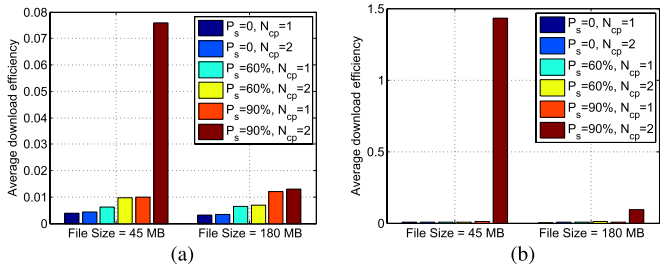


Fig. 12. Average download efficiency. (a) The number of vehicles=50. (b) The number of vehicles=100.

In reality, the client vehicle probably exits the highway after a period of time; therefore the packets would not be delivered to the client vehicle completely. If the client vehicle cannot receive all packets, it may not recover the file content successfully. Therefore, all the packets should be delivered to the client vehicle as soon as possible in case the client vehicle leaves from the highway at any time. Therefore, we define the average download efficiency (ADE) as

$$ADE = \frac{Average\ download\ success\ rate}{Average\ download\ delay} \tag{15}$$

The greater ADE indicates that more packets can be delivered to the client vehicle within minimum delay. We further plot Fig. 12 (a) and Fig. 12 (b) to analyze the average download efficiency on different conditions. From Fig. 12 (a) and Fig. 12 (b), we can observe two facts: 1) When same incentives are applied, the average download efficiency of the 2-copy case is better than that of the 1-copy case; 2) when forwarding the same number of packet copies, the more the incentive is applied, the higher the average download efficiency is. Especially, when the high incentive and the multi-copy forwarding are adopted at the same time, the average download efficiency is far better than that of other cases.

VII. Conclusions

In this paper, we have proposed a secure incentive scheme (SIRC) to reliably, fairly and securely achieve the cooperative downloading in VANETs. By adopting the "virtual checks" and partial prepayment strategy, the proposed SIRC scheme can achieve the fairness among vehicle users and minimize the payment risk of the client vehicle. In addition, we have proposed a multi-path forwarding scheme with reputation-based incentive to further enhance the reliability. Security analysis has shown that SIRC can resist various attacks launched by selfish vehicle users, including injection/removing attack, free riding attack, DoS attacks. Moreover, the privacy of the client vehicle can be preserved. Extensive simulation results have demonstrated that SIRC achieves the higher download success rate but lower average download delay when simultaneously applying the high incentive and muti-path forwarding. For our future work, we will integrate SIRC with anonymity and carry out experiments in the testing platforms to further verify the effectiveness of the proposed SIRC scheme.

References

[1] L. Wischhof, A. Ebner, and H. Rohling, "Information dissemination in self-organizing intervehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 6, no. 1, pp. 90–101, Mar. 2005.

[2] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Mar. 2012.

[3] S. Taha and X. Shen, "A physical-layer location privacy-preserving scheme for mobile public hotspots in NEMO-based VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 4, pp. 1665–1680, Dec. 2013.

[4] N. Lu, N. Zhang, N. Cheng, X. Shen, J. W. Mark, and F. Bai, "Vehicles meet infrastructure: Toward capacity–cost tradeoffs for vehicular access networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 3, pp. 1266–1277, Sep. 2013.

[5] T. H. Luan, X. S. Shen, and F. Bai, "Integrity-oriented content transmission in highway vehicular ad hoc networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2562–2570.

[6] X. Zhuo, W. Gao, G. Cao, and S. Hua, "An incentive framework for cellular traffic offloading," *IEEE Trans. Mobile Comput.*, vol. 13, no. 3, pp. 541–555, Mar. 2014.

[7] J. Ott and D. Kutscher, "Drive-thru Internet: IEEE 802.11b for 'automobile' users," in *Proc. IEEE INFOCOM*, Mar. 2004, pp. 362–373.

[8] T. H. Luan, X. Ling, and X. Shen, "MAC in motion: Impact of mobility on the MAC of drive-thru Internet," *IEEE Trans. Mobile Comput.*, vol. 11, no. 2, pp. 305–319, Feb. 2012.

[9] W. Saad, Z. Han, A. Hjorungnes, D. Niyato, and E. Hossain, "Coalition formation games for distributed cooperation among roadside units in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 1, pp. 48–60, Jan. 2011.

[10] H. Liang and W. Zhuang, "Cooperative data dissemination via roadside WLANs," *IEEE Commun. Mag.*, vol. 50, no. 4, pp. 68–74, Apr. 2012.

[11] H. Zhou *et al.*, "ChainCluster: Engineering a cooperative content distribution framework for highway vehicular communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 6, pp. 2644–2657, Dec. 2014.

[12] T. Ning, Z. Yang, H. Wu, and Z. Han, "Self-interest-driven incentives for ad dissemination in autonomous mobile social networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2310–2318.

[13] Y.-D. Lin and Y.-C. Hsu, "Multihop cellular: A new architecture for wireless communications," in *Proc. 19th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM)*, vol. 3. Mar. 2000, pp. 1273–1282.

[14] K. Fall, "A delay-tolerant network architecture for challenged Internets," in *Proc. SIGCOMM*, 2003, pp. 27–34.

[15] M. M. E. A. Mahmoud and X. Shen, "FESCIM: Fair, efficient, and secure cooperation incentive mechanism for multihop cellular networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 5, pp. 753–766, May 2012.

[16] M. M. E. A. Mahmoud and X. Shen, "A secure payment scheme with low communication and processing overhead for multihop wireless networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 2, pp. 209–224, Feb. 2013.

[17] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A secure multilayer credit-based incentive scheme for delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 8, pp. 4628–4639, Oct. 2009.

[18] R. Lu, X. Lin, H. Zhu, X. Shen, and B. Preiss, "Pi: A practical incentive protocol for delay tolerant networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1483–1493, Apr. 2010.

[19] S. M. Tornell, C. T. Calafate, J. C. Cano, and P. Manzoni, "DTN protocols for vehicular networks: An application oriented overview," *IEEE Commun. Surveys Tut.*, vol. 17, no. 2, pp. 868–887, 2015.

[20] A. Agarwal, D. Starobinski, and T. D. C. Little, "Phase transition of message propagation speed in delay-tolerant vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 249–263, Mar. 2012.

[21] M. J. Khabbaz, H. M. K. Alazemi, and C. M. Assi, "Delay-aware data delivery in vehicular intermittently connected networks," *IEEE Trans. Commun.*, vol. 61, no. 3, pp. 1134–1143, Mar. 2013.

[22] M. Liang, Z. Zhang, C. Liu, and L. Chen, "Multihop-delivery-quality-based routing in DTNs," *IEEE Trans. Veh. Technol.*, vol. 64, no. 3, pp. 1095–1104, Mar. 2015.

[23] A. Nandan, S. Das, G. Pau, M. Gerla, and M. Y. Sanadidi, "Co-operative downloading in vehicular ad-hoc wireless networks," in *Proc. IEEE WONS*, Jan. 2005, pp. 32–41.

[24] I. Leontiadis, P. Costa, and C. Mascolo, "Extending access point connectivity through opportunistic routing in vehicular networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–5.

[25] O. Trullols-Cruces, M. Fiore, and J. Barcelo-Ordinas, "Cooperative download in vehicular environments," *IEEE Trans. Mobile Comput.*, vol. 11, no. 4, pp. 663–678, Apr. 2012.

[26] J. Liu, J. Bi, Y. Bian, X. Liu, and Z. Li, "DSRelay: A scheme of cooperative downloading based on dynamic slot," in *Proc. IEEE ICC*, Jun. 2012, pp. 381–386.

[27] Y. Hao, J. Tang, and Y. Cheng, "Secure cooperative data downloading in vehicular ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 523–537, Sep. 2013.

[28] X. Cheng, C.-X. Wang, B. Ai, and H. Aggoune, "Envelope level crossing rate and average fade duration of nonisotropic vehicle-to-vehicle Ricean fading channels," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 1, pp. 62–72, Feb. 2014.

[29] X. Cheng, Q. Yao, M. Wen, C.-X. Wang, L.-Y. Song, and B.-L. Jiao, "Wideband channel modeling and intercarrier interference cancellation for vehicle-to-vehicle communication systems," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 434–448, Sep. 2013.

[30] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 289–299, Aug. 2014.

[31] X. Cheng, L. Yang, and X. Shen, "D2D for intelligent transportation systems: A feasibility study," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 1784–1793, Aug. 2015.

[32] F. Li, J. Wu, and A. Srinivasan, "Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 2428–2436.

[33] S. Saeednia, S. Kremer, and O. Markowitch, "An efficient strong designated verifier signature scheme," in *Proc. ICISC*, 2004, pp. 40–54.

[34] K. Lee, D. Lee, and M. Yung, "Aggregating cl-signatures revisited: Extended functionality and better efficiency," in *Proc. Int. Conf. Financial Cryptography Data Secur.*, 2013, pp. 171–188.

[35] K. Zhang, X. Liang, R. Lu, and X. Shen, "Exploiting private profile matching for efficient packet forwarding in mobile social networks," in *Handbook on Opportunistic Mobile Social Networks*. Boca Raton, FL, USA: CRC, 2014, pp. 283–311.

[36] R. Lu, X. Lin, and X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1229–1237.

[37] B. J. Matt, "Identification of multiple invalid signatures in pairing-based batched signatures," in *Proc. PKC*, 2009, pp. 337–356.

[38] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[39] B. Lynn. (2012). *PBC Library*. [Online]. Available: http://crypto.stanford.edu/pbc/

[40] S. Skiena. (2012). *Multiprecision Integer and Rational Arithmetic C/C++ Library*. [Online]. Available: http://www.shamus.ie/

[41] J. Härri, F. Filali, C. Bonnet, and M. Fiore, "VanetMobiSim: Generating realistic mobility patterns for VANETs," in *Proc. VANET*, 2006, pp. 96–97.

[42] M. Fiore, J. Harri, F. Filali, and C. Bonnet, "Vehicular mobility simulation for VANETs," in *Proc. ANSS*, 2007, pp. 301–309.

[43] *Geography*, US Census Bureau, accessed on Sep. 28, 2016. [Online]. Available: http://www.census.gov/geo/maps-data/data/tiger.html

[44] J. Harri and M. Fiore, "VanetMobiSim–vehicular ad hoc network mobility extension to the CanuMobiSim framework," Dept. Mobile Commun. Inst. Eurecom, Sophia Antipolis, France, Tech. Rep., 2006, vol. 6904.

Chengzhe Lai (M'15) received the B.S. degree in information security from Xi'an University of Posts and Telecommunications in 2008 and the Ph.D. degree from Xidian University in 2014. He was a Visiting Ph.D. Student with the Broadband Communications Research Group, University of Waterloo, from 2012 to 2014. He is currently with the School of Telecommunication and Information Engineering, Xi'an University of Posts and Telecommunications, and also with the National Engineering Laboratory for Wireless Security, Xi'an, China. He is also a Visiting Researcher with State Key Laboratory of Integrated Services Networks and the State Key Laboratory of Information Security. His research interests include wireless network security, privacy preservation, and VANET security.

Kuan Zhang (S'13) received the B.Sc. degree in communications engineering and the M.Sc. degree in computer science from Northeastern University, China, in 2009 and 2011, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Canada, in 2016.

He is currently a Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research interests include security and privacy for mobile social networks, e-healthcare system, and cloud computing.

Nan Cheng (S'13) received the B.S. and M.S. degrees from Tongji University, China, in 2009 and 2012, respectively, and the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2016. He is currently a Research Engineer with the Huawei Technology Canada Research Center, Ottawa, ON, Canada. His research interests include vehicular communication networks, cellular traffic offloading, cognitive radio networks, and device-to-device communications.

Hui Li (M'10) received the B.Sc. degree from Fudan University in 1990, and the M.Sc. and Ph.D. degrees from Xidian University, China, in 1993 and 1998, respectively. In 2009, he was with the Department of Electronic and Communication Engineering, University of Waterloo, as a Visiting Scholar. Since 2005, he has been a Professor with Xidian University. He is currently the Executive Dean with the School of Cyber Engineering and the Dean with the School of International Education. His research interests are in the areas of cryptography, wireless network security, cloud computing security, privacy preservation, and information theory. He has authored over 160 papers in academic journals and conferences. He served as the TPC Co-Chair of the ISPEC 2009 and the IAS 2009, the General Co-Chair of the E-Forensic 2010, the ProvSec 2011, and the ISC 2011, and the Honorary Chair of the NSS 2014 and the ASIACCS 2016.

Xuemin Shen (M'97–SM'02–F'09) received the B.Sc. degree from Dalian Maritime University, China, in 1982, and the M.Sc. and Ph.D. degrees in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 1987 and 1992, respectively. He is currently a Professor and a University Research Chair with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is also an Associate Chair for Graduate Studies. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular *ad hoc* and sensor networks. He is an Elected Member of the IEEE ComSoc Board of Governor and the Chair of Distinguished Lecturers Selection Committee. He served as the Technical Program Committee Chair/Co-Chair for the IEEE GLOBECOM'16, the InfoComm'14, the IEEE VTC'10 Fall, and the GLOBECOM'07, the Symposia Chair for the IEEE ICC'10, the Tutorial Chair for the IEEE VTC'11 Spring and the IEEE ICC'08, the General Co-Chair for the ACM MobiHoc'15, the CHINACOM'07, and the QShine'06, and the Chair for the IEEE Communications Society Technical Committee on Wireless Communications and P2P Communications and Networking. He also serves/served as the Editor-in-Chief for IEEE Network, Peer-to-Peer Networking and Application, and IET Communications. He is a Founding Area Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, an Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, COMPUTER NETWORKS, and ACM/Wireless Networks, and the Guest Editor for IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS, IEEE *Communications Magazine*, and *ACM Mobile Networks and Applications*. He received the Excellent Graduate Supervision Award in 2006; the Outstanding Performance Award from University of Waterloo in 2004, 2007, 2010, and 2014; the Premier's Research Excellence Award from the Province of Ontario, Canada, in 2003; and the Distinguished Performance Award from the Faculty of Engineering, University of Waterloo, in 2002 and 2007. He is a Registered Professional Engineer of Ontario, Canada. He is an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society.