SPRING: A Social-based Privacy-preserving Packet Forwarding Protocol for Vehicular Delay Tolerant Networks

Rongxing Lu, Xiaodong Lin, Xuemin (Sherman) Shen
Date Submitted: 7 August 2009
Date Published: 9 August 2009

Updated information and services can be found at:

These include:

Subject Classification  Vehicular Technology

Keywords  Vehicular DTNs; Social-based RSU placement; RSU-aided packet forwarding; Conditional privacy preserving;

Submitting Author's Comments  The paper has been submitted to INFOCOM 2010.

Comments  You can respond to this article at:
https://preprint.lib.uwaterloo.ca/ojs-2.2/index.php/pptvt/comment/add/547/0

Copyright  Copyright © Date Submitted: 7 August 2009 Rongxing Lu et al.  This is an open access article distributed under the Creative Commons Attribution 2.5 Canada License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.
SPRING: A Social-based Privacy-preserving Packet Forwarding Protocol for Vehicular Delay Tolerant Networks

Rongxing Lu†, Xiaodong Lin‡, and Xuemin (Sherman) Shen†
†Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
‡Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, Ontario, Canada
Email: {rxlu, xshen}@bber.uwaterloo.ca; xiaodong.lin@uoit.ca

Abstract—In this paper, we propose a social-based privacy-preserving packet forwarding protocol, called SPRING, for vehicular delay tolerant networks (DTNs). With SPRING, Roadside Units (RSUs) deployed along the roadside can assist in packet forwarding to achieve highly reliable transmissions. In specific, we first heuristically define how to evaluate each traffic intersection's social degree in a vehicular DTN. Based on the social degree information, we then strategically place RSUs at some high-social intersections. As a result, these RSUs can provide tremendous assistance in temporarily storing packets and helping packet forwarding to achieve high delivery ratio. Performance evaluations via extensive simulations demonstrate the SPRING's efficiency. In addition, detailed security analyses show that the proposed SPRING can achieve conditional privacy preservation and resist most attacks existing in vehicular DTNs.

Keywords – Vehicular DTNs; Social-based RSU placement; RSU-aided packet forwarding; Conditional privacy preserving

I. INTRODUCTION

In recent years, Delay tolerant networks (DTNs), such as space communication and networking in sparsely populated areas [1], vehicular ad hoc networks [2], have been subject to extensive research efforts. Unlike traditional tethered networks like the Internet, a DTN is a sparse mobile network where the connection between nodes in the network changes over time, and as a result the communication constantly suffers from higher delays and disconnections. Since a contemporaneous end-to-end path may never exist in DTNs, effective communication in DTNs requires cooperation of all the nodes for routing and forwarding, where, the intermediate nodes on a communication path are expected to store, carry and forward the packets in an opportunistic way, which is also named as opportunistic data forwarding. However, in most cases, DTNs could consist of many resource-constrained nodes, i.e., limited storage. If carried for a certain of time without an available downstream node, the packets have to be dropped by the carrying node, which thus incurs very unreliable forwarding in DTNs. Therefore, efficient packet forwarding in DTNs becomes an especially challenging issue, and a number of DTN packet forwarding schemes recently have been proposed to improve the reliability [3].

Over the past few years, vehicular ad hoc network, as a special case of DTNs and also known as vehicular DTN, has become increasingly attractive to the public due to its promising ability of improving road safety and traffic efficiency. In vehicular networks, a variety of applications can be enabled by vehicle-to-vehicle (V-2-V) and vehicle-to-infrastructure (V-2-I) communications to improve transportation systems. Unlike other forms of DTNs, there exists a fixed infrastructure in VANETs, i.e., Roadside Units (RSUs) deployed along the roadside. Recent efforts to improve the reliability of DTNs show that the introduced infrastructure in DTNs could dramatically enhance wireless networks in terms of packet delivery ratio [4]. Obviously, it is viable to adopt an RSU-aided packet forwarding mechanism in VANETs, where RSUs are used to assist in forwarding packets. However, deploying infrastructure is very costly, preventing from making RSUs widely available, for example, in rural areas or in the early stage deployment phase of VANET. Thus, effectively deploying RSUs is crucial to improving packet forwarding efficiency in VANETs. Heavy traffic is a common occurrence in some areas on the roads, for example, at intersections, Taxi loading/unloading areas. Despite dynamics of traffic flow, traffic pattern is relatively static in an area. For example, during morning rush hours, overwhelming traffic can be observed inside a certain area, such as, in the downtown area because of its core focus on business. In other words, the area becomes a popular social place for vehicles to connect to each other. Obviously, if a roadside infrastructure is deployed in these high traffic areas and then used to assist in forwarding data packets in VANETs, reliability in vehicular communications can be dramatically improved with incurred costs under control. Furthermore, security and privacy issue is crucial to the full adoption of any networks, but security and privacy issues in DTN have been subject to little attention.

Based on the above observations, in this paper, we propose a novel Social-based PRivacy-preserving packet forwarding (SPRING) protocol for vehicular DTNs. The proposed SPRING protocol is characterized by deploying RSUs at high social intersections to assist in packet forwarding between vehicles by temporarily storing packets through V-2-I communication during the period when the proper next-hop vehicles of these packets are not available. With such kind of RSU assistance, the probability of packet drop is reduced and as a result high reliability of packet forwarding in vehicular DTNs can be achieved. Specifically, the contributions of this paper are threefold.

First, we heuristically define the social degree of intersections in vehicular DTNs. Based on the social information, we place RSUs at these high social intersections. To the best of
our knowledge, this is the first attempt to investigate social-based RSU deployment in vehicular DTNs.

Second, we propose the SPRING protocol, a social-based privacy-preserving packet forwarding protocol for vehicular DTNs. In SPRING, because the stationary RSUs are deployed at high social intersections, a large number of vehicles will pass by these RSUs. Then, RSUs can provide tremendous assistance in temporarily storing some packets and helping packet forwarding to achieve high transmission reliability. In addition, SPRING can also achieve conditional privacy preservation and resist most attacks existing in vehicular DTNs, such as packet analysis attack, packet tracing attack, and black (grey) hole attacks [5], which is crucial to success of such networks.

Third, we develop a simulator to show the substantial improvement of the SPRING protocol in terms of high reliability, resistance to packet tracing attack, and black (grey) hole attacks. The simulation results demonstrate its effectiveness and security.

The remainder of this paper is organized as follows. In Section II, we formalize the network, node and threat models and identify our design goal. Then, we present the SPRING protocol in Section III, followed by the security analysis and performance evaluation in Section IV and Section V, respectively. We also review related works in Section VI. Finally, we draw our conclusions in Section VII.

II. MODELS AND DESIGN GOAL

In this section, we formalize the network model, node model and threat model, and as well identify our design goal.

A. Random Graph-Based Network Model

Consider a large number of vehicles $\mathcal{V} = \{v_1, v_2, \cdots\}$ moving around in a city by following map-based shortest path routing algorithm. Then, a vehicular DTN can be represented as a directed random graph $\mathcal{G} = (\mathcal{V}^*, \mathcal{E})$, as shown in Fig. 1(a), where $\mathcal{V}^*$ is a union between the set of vehicle nodes $\mathcal{V}$ and a set of intersection nodes $\mathcal{C} = \{c_1, c_2, \cdots\}$, i.e., $\mathcal{V}^* = \mathcal{V} \cup \mathcal{C}$, and $\mathcal{E}$ is the set of directed random edges between any intersections $c_i, c_j \in \mathcal{C}$, where $i \neq j$. For any edge $e_{ij} \in \mathcal{E}$ from $c_i$ to $c_j$, we denote the flow of $e_{ij}$ as $F(e_{ij}) = \sigma_{ij} \cdot \lambda_{ij}$, where $\sigma_{ij} = 1$ if $c_i, c_j$ are connected by a direct road (i.e., no intermediate intersection between $c_i$ and $c_j$), and 0 otherwise; $\lambda_{ij}$ is the Poisson arrival rate of the road $(c_i \rightarrow c_j)$ if $\sigma_{ij} = 1$ and assuming the arrival follows the Poisson distribution, which can realistically capture the average number of vehicles passing from $c_i$ to $c_j$ during a unit of time. If $F(e_{ij}) = 0$, the edge $e_{ij}$ doesn’t exist. Note that in reality, $\sigma_{ij} = \sigma_{ji}$, while $\lambda_{ij}$ may differ from $\lambda_{ji}$.

In-Degree of interaction vertex $c_i \in \mathcal{C}$ is the number of roads with $c_i$ as their terminal vertex, and is denoted as $KI_i = \sum_{j \in \mathcal{C}} \sigma_{ji}$. Out-Degree of interaction vertex $c_i \in \mathcal{C}$ is the number of roads with vertex $c_i$ as their initial vertex, and is denoted as $KO_i = \sum_{j \in \mathcal{C}} \sigma_{ij}$. Because $\sigma_{ji} = \sigma_{ij}$, we have $KI_i = KO_i$. Generally, in a directed graph, both degree and out-degree of a vertex can capture its impact in the whole graph. However, in the defined random directed graph, the impact of an interaction vertex $c_i$ is contingent upon the number of contacts between $c_i$ and other vehicle nodes in $\mathcal{V}$. Therefore, the Social Degree of interaction vertex is introduced.

Social Degree of an intersection vertex $c_i \in \mathcal{C}$ is defined as

$$SD_i = \frac{\sum_{v_j \in \mathcal{V}} \delta_j(c_i)}{\sum_{v_j \in \mathcal{V}} \delta_j}$$

where $\delta_j$ is the number of shortest paths that a vehicle node $v_j \in \mathcal{V}$ drives during a unit of time, and $\delta_j(c_i)$ is the number of shortest paths that passes through the intersection vertex $c_i$.

In the defined random graph, it is easy to show that, for any intersection vertex $c_i \in \mathcal{C}$, $\sum_{e_{ij} \in \mathcal{E}, \sigma_{ij} = 1} \lambda_{ij} = \sum_{c_i \in \mathcal{C}, \sigma_{ij} = 1} \lambda_{ij}$, although $\lambda_{ji} \neq \lambda_{ij}$ for some $c_j$. With this observation, the flow of the intersection vertex $c_i$ can be defined as $F(c_i) = \sum_{c_j \in \mathcal{C}} F(e_{ij}) = \sum_{c_j \in \mathcal{C}} \sigma_{ij} \cdot \lambda_{ij}$. Because all vehicles $V = \{v_1, v_2, \cdots\}$ follow the map-based shortest path routing, the social degree $SD_i$ of $c_i$ can be rewritten as

$$SD_i = \frac{F(c_i)}{\sum_{e_{ij} \in \mathcal{E}} \delta_j} = \frac{\sum_{c_j \in \mathcal{C}} \sigma_{ij} \cdot \lambda_{ij}}{\sum_{v_j \in \mathcal{V}} \delta_j}$$

Deployment of RSUs. Let $ST$ denote the social threshold of a given random directed graph $\mathcal{G} = (\mathcal{V}^* \mathcal{E})$. We choose a set of high social intersection vertexes as follows

$$HS = \{c_i \in \mathcal{C} | SD_i \geq ST\}$$

Note that, by adjusting the social threshold $ST$, we can determine the cardinality of $HS$. After the set $HS$ is determined, we place an RSU $R_i$ at each intersection $c_i \in HS$, as shown in Fig. 1(b). Then, each RSU has high social capability and can effectively assist vehicles to store-forward packets in vehicular DTNs.

B. Node Model

Vehicular DTNs, as distinct from general DTNs, are characterized by two kinds of DTN nodes, i.e., vehicles and RSUs, each kind of which has unique characteristics.

- Vehicles: Apart from the mobility, each vehicle node is also resource-constrained, i.e., buffer constraints. In general, a vehicle node will help forwarding the packets when it has available storage. However, once the storage is insufficient, the vehicle node no longer serves the relay node to help forwarding.
• **Roadside Units (RSUs):** Different from the vehicle node, each RSU node is stationary but has huge storage capacity. Once it is deployed at some intersection, each RSU node can temporarily help store some bundle packets till passing-by vehicle nodes carry them close to their destinations. However, since each RSU is costly, it is impractical to erect RSU nodes at all intersections, especially at the early deployment of VANETs. Therefore, as discussed in the network model, only a small number of RSU nodes will place at some high social intersections.

Let $T_R$ and $T_V$, where $T_R > T_V$, be the transmission ranges of RSU and vehicle nodes, respectively. Then, the wireless interfaces between vehicle nodes are bidirectional, i.e., if $v_i$ hears the transmission of $v_j$, then $v_j$ can also hear $v_i$. However, the wireless interfaces between vehicle node and RSU node are usually unidirectional unless they are very close to each other, as shown in Fig. 2. Therefore, packets in vehicular DTNs will be i) either stored-carried by the vehicle nodes or stored in RSU nodes if no other node is encountered; ii) forwarded when other node is encountered.

### C. Threat Model

In our threat model, RSU nodes are trustable, and non-compromisable. However, a small fraction of vehicle nodes may be compromised. We consider a global external adversary $A$ with limited control capability, where

- **Global** shows the adversary $A$ has full traffic information of the whole vehicular DTN;
- **External** denotes the adversary $A$ generally can only capture the communications between DTN nodes, but has no idea about the internal information stored in these nodes.
- **Limited control** means the adversary $A$ can control a very small fraction, (i.e., $< 10\%$), of vehicle nodes to launch some kinds of active attacks. (Note that, limited controlling a small fraction of vehicles nodes doesn’t help the adversary $A$ to gain other vehicles’ key materials.)

In specific, we consider the adversary $A$ can launch the following attacks to either subvert privacy or degrade the performance of the whole vehicle DTN.

- **Packet analysis attack:** After eavesdropping a packet, the adversary $A$ tries to identify the source identity by analyzing the packet, i.e., recover the packet content and infer the source.
- **Packet tracing attack:** The adversary $A$ eavesdrops the transmission of a single packet as it traverses around the vehicular DTN. In such a way, the source and destination locations of the packet can be traced. Note that the adversary $A$ doesn’t need to recover the packet content to infer the source and destination locations of the flow.

- **Black hole attack:** In vehicular DTN, the adversary $A$ first lures packets by claiming that it can help forward them close to their destinations. However, all packets are actually dropped by the adversary $A$. Clearly, the black hole attack is one kind of Denial of Service (DoS) attacks, which can largely degrade the performance of the whole vehicular DTN, especially when the adversary $A$ controls some compromised vehicle DTN nodes to launch the attack.

- **Grey hole attack:** Grey hole attack is a variant of black hole attack in vehicular DTN, where the adversary $A$ selectively forwards some packets but not all packets. This kind of attack is hardly to detect because it is indistinguish from the normal packet dropping event when the vehicular DTN is poor-connected.

### D. Design Goal

Under the above models, our design goal in this paper is to develop a social-based privacy-preserving packet forwarding protocol for vehicular DTNs. Specifically, the following three desirable objectives will be achieved.

- **Optimizing vehicular DTN with RSU assistance.** In a large vehicular DTN, when the vehicle density is sparse, the contacting opportunity of vehicle DTN nodes is low, which will incur the low delivery ratio in vehicular DTN, especially when the single-copy technique is adopted. In order to prevent the overall performance degradation, we introduce high social RSU deployment into vehicular DTNs. Because RSUs have huge storage capabilities, they can temporarily store packets when the next-hop vehicle node is not available. In addition, the high social capacities of these RSUs can ensure they can contact many more vehicles in a very short time. As a result, the delay due to RSU temporary storing can be confined, and the performance of the vehicular DTN is optimized.

- **Resisting privacy-related attacks on vehicle DTN nodes.** Because vehicular DTN is usually implemented in civilian scenarios, where the locations of vehicle nodes are tightly related to the citizens who are driving them. If the vehicular DTN discloses the privacy information of the citizens, i.e., identity and location privacy, vehicular DTN can’t be widely accepted by the public. Therefore, the citizens’ privacy must be protected in order for wide acceptance to the public.

- **Achieving conditional privacy preservation:** Following the threat model discussed earlier, if the adversary $A$ launches the black/grey hole attacks by controlling a small fraction of compromised vehicle nodes, these attacks are hard to resist, because these compromised nodes have their valid key materials. Therefore, the absolute privacy preservation is insufficient, and the conditional privacy preservation is expected. In specific, once a
compromised vehicle node launches the attack, a trust authority (TA) should have ability to identify the compromised node and punish it under the applicable law.

III. PROPOSED SPRING PROTOCOL

In this section, we present our social-based privacy-preserving packet forwarding (SPRING) protocol for vehicular DTNs, which mainly consists of the following two phases: system initialization phase and opportunistic RSU-aided packet forwarding phase. Before delving into the details of our protocol, we first review a conditional privacy-preserving authentication (CPPA) technique [6], which serves as the basis of the proposed SPRING protocol.

A. Conditional Privacy-preserving Authentication Technique

The CPPA technique is one kind of group signature [7], which is dedicated for vehicular communications to achieve conditional privacy-preserving authentication. Concretely, it includes the following three parts: system initialization, privacy-preserving authentication, and conditional tracking.

1) System Initialization: Let $G$, $G'$ and $G_T$ be three cyclic groups of the same large prime order $q$. Suppose $G$, $G'$ and $G_T$ are equipped with a pairing, i.e., a non-degenerated and efficiently computable bilinear map $e : G \times G' \rightarrow G_T$ such that $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ for all $a, b \in \mathbb{Z}_q^*$ and any $g_1 \in G$, $g_2 \in G'$. Let $g$, $g'$ be the generators of $G$, $G'$, respectively, and $\psi$ be an isomorphism from $G'$ to $G$, with $\psi(g') = g$ and $e(g, g') \neq 1_{G_T}$. A trusted authority (TA) chooses two random numbers $u, v \in \mathbb{Z}_q^*$ as the master-key, and computes $U' = g^u$, $U = g^v$, and $V = g^v$. In addition, the TA also chooses a secure cryptographic hash function: $H : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$, and a secure symmetric encryption algorithm $Enc()$. Then, the system parameters $params = \{q, G, G', G_T, e, g, g', g, U', U, V, H, Enc()\}$ are published.

Once a vehicle $v_i$ with identity $ID_{v_i}$ wants to register with the system, the TA executes the following steps: i) choose a random number $r_i \in \mathbb{Z}_q^*$ such that $r_i + u \neq 0 \mod q$ and compute $A_i = g^{r_i+u}$; ii) store the duplet $(ID_{v_i}, A_i^u)$ in the tracing list and return $(x_i, A_i)$ as the secret key to $v_i$.

2) Privacy-preserving Authentication: Assume that the vehicle $v_i$ wants to anonymously authenticate itself at time $T_i$, it uses the secret key $(x_i, A_i)$ to execute the following steps:

- Randomly choose $\alpha, r_{\alpha}, r_x, r_\delta \in \mathbb{Z}_q^*$ and compute $T_U, T_V, \delta, \delta_1, \delta_2, \delta_3$, where $T_U = U^\alpha$, $T_V = A_i \cdot V^\alpha$, $\delta = \alpha \cdot x_i \mod q$, $\delta_1 = T_U^r$, $\delta_2 = T_V^{r_x}$, $\delta_3 = e(T_U, g^{r_\delta})/e(V, U^{\delta_2} \cdot g^{\delta_3})$;
- Compute $c = H(U||V||T_U||T_V||T_U||T_V||\delta) \in \mathbb{Z}_q^*$ and $s_a$, $s_x, s_\delta \in \mathbb{Z}_q^*$, where $s_a = r_{\alpha} + c \cdot \alpha \mod q$, $s_x = r_x + c \cdot r_i \mod q$, $s_\delta = r_\delta + c \cdot \delta \mod q$;
- Set CPPA($T_i$) = $(T_i; T_U||T_V||c||s_a||s_x||s_\delta)$ as the authentication information.

After receiving CPPA($T_i$) at time $T_i'$, any verifier checks whether or not $T_i' - T_i \leq \Delta T$, where $\Delta T$ is the expected legal time interval for transmission delay. If it doesn’t hold, the authentication fails. Otherwise, the verifier executes the following steps:

- Compute $\delta_1' = U^{s_a}/T_U^{r_x}$, $\delta_2' = T_V^{s_x}/T_V^{\delta_2}$, $\delta_3' = e(T_V, g^{s_\delta} \cdot U^{\delta_3})/e(V, U^{s_x} \cdot g^{\delta_3})$;
- Check whether $c = H(U||V||T_i)||T_i||\delta_1||\delta_2||\delta_3)$ if it holds, the vehicle $v_i$ is anonymously authenticated, i.e., $v_i$ is a valid registered user in the system, but the real identity is not disclosed; Otherwise the authentication fails. The corrections are as follows: $\delta_1' = U^{s_a}/T_U^{r_x} = U^{r_x + \alpha}/U^{\alpha} = \delta_1$; $\delta_2' = T_V^{s_x}/T_V^{\delta_2} = T_V^{r_x + \delta_2}/U^{\delta_2 + \delta_3} = \delta_2$; $\delta_3' = e(T_V, g^{s_\delta})e(V, U^{s_x} \cdot g^{\delta_3}) = \delta_3$.

3) Conditional Tracking: Once the dispute occurs, the TA can fast track the real identity of vehicle with CPPA($T_i$) as follows:

- Use the master key $(u, v)$ to compute $T_U^u/T_V^u = A_i^u$, $V^{uo}/U^{vo} = A_i^u \cdot g^{uo}/g^{vo} = A_i^u$.
- By seeking the entry $(ID_{v_i}, A_i^u)$ in the tracing list with condition $A_i^u$, the TA can easily find the real identity $ID_{v_i}$ of vehicle $v_i$. As a result, the CPPA technique achieves conditional privacy-preserving authentication. Note that during the conditional tracking, no pairing computation is needed, the tracking is faster than other previously reported ones [7].

B. Description of the SPRING Protocol

1) System Initialization Phase: Based on the system requirements, the following steps are performed to bootstrap the whole system:

- Assume that there exists a trust authority (TA) in the system, which first chooses two random numbers $u, v \in \mathbb{Z}_q^*$ as the master-key and generates the system parameters $params = \{q, G, G', G_T, e, g, g', g, U', U, V, H, Enc()\}$ as above.
- For each vehicle $v_i \in V = \{v_1, v_2, \cdots\}$, the TA chooses a random number $x_i \in \mathbb{Z}_q^*$ such that $x_i + u \neq 0 \mod q$ as a secret key, and computes $A_i = g^{r_i+u} \in G$, $B_i = g^{x_i} \in G_T$. Then, TA sets $(x_i, A_i)$ as $v_i$’s anonymous credential and stores duplet $(v_i, A_i^u)$ in the tracing list. In addition, TA authorizes $B_i \in G_T$ as the public key of $v_i$.
- For a specific area, the TA first investigates a set of intersection nodes $C = \{c_1, c_2, \cdots\}$ and computes the social degree $SD_j$ of each intersection $c_j$. Then, by setting a social threshold $ST$, the TA derives a set of high social intersection nodes $HS = \{c_i \in C|SD_i > ST\}$. At each high social intersection, TA places an RSU, authorizes a secret key $x_j \in \mathbb{Z}_q^*$ and the corresponding public key $C_j = g^{x_j} \in G_T$ for the RSU. Note that the public key $C_j$ here is associated with the intersection $c_i$ attested with a certificate issued by the TA.

2) Opportunistic RSU-aided packet forwarding phase: Suppose that a source node $v_1$ wants to send a sensitive message $m \in G_T$ to the destination node $v_2$, where the location $L_2$ of $v_2$ is assumed stationary and known by $v_1$. To fulfill such sensitive packet forwarding in vehicular DTN, the following steps will be executed.

Step 1. The source node $v_1$ first uses the destination node $v_2$’s public key $B_2 = g^{x_2}$ and two random numbers $k_0, k_1 \in \mathbb{Z}_q^*$ to execute the following steps:
\[ M = (\alpha_0, \beta_0, \alpha_1, \beta_1) = (m \cdot B_2^{k_0}, g^{k_0}, B_2^{k_1}, g^{k_1}) \] (4)

The latter part of ciphertext \((\alpha_1, \beta_1)\) will be used for any future possible re-encryption on \(M\) by RSUs in order to build up a mix network \[8\].

**Step 2.** When a passing-by vehicle node \(v_i\) is willing to help forwarding the message \(M\), the source node \(v_1\) and node \(v_i\) execute the following interactive operations.

- **The passing-by vehicle** \(v_i\) first gets the current timestamp \(T_i\) and computes \(g^x\) where \(x\) is randomly chosen from \(Z_q^*\). Then, \(v_i\) uses the CPA technique to construct \(\text{CPPA}(T_i||g^x)\) and sends it to the source node \(v_1\).
- **After checking the validity of \(\text{CPPA}(T_i||g^x)\), \(v_i\) chooses another random number \(y \in Z_q^*\), encrypts the destination location \(L_2\) as \(D = (\alpha_2, \beta_2) = (L_2 \cdot g^{x y}, g^y)\), and sends \(M||D\) back to the passing-by vehicle \(v_1\).
- **After recovering the destination location \(L_2\) from \(D = (\alpha_2, \beta_2)\) as \(\alpha_2 = g^{x y} \in Z_q^*\), the passing-by vehicle \(v_i\) tries its best to help carrying the message \(M\) closer to the destination.

**Step 3.** After the vehicle \(v_i\) carries the message \(M\) for a period of time, the destination \(L_2\) is no longer on the way of the vehicle \(v_i\)’s way. Then, \(v_i\) invokes the Algorithm 1 to forward the message \(M\) to a proper next-hop node. Because RSU’s transmission range \(T_R\) is larger than vehicle’s transmission range \(T_V\), if there exists an RSU at some nearby intersection \(c_i\) on its way, the vehicle \(v_i\) can first detect it. Then, \(v_i\) will drive close to the RSU and forward the message \(M\) with V-2-I communication as follows.

**Algorithm 1:** Packet forwarding in vehicular DTN

1: procedure PACKET FORWARDING
2: when the vehicle node \(v_i\) thinks it can’t help carrying message \(M\) any more, it will first set a holding time to wait next-hop node \(T_h\) and try to forward \(M\) to the next-hop DTN node within \(T_h\)
3: \(v_i\) will drive close and forward the message \(M\) to the RSU, \(v_j\) detects an available vehicle node \(v_i\) nearby then
4: \(v_i\) will forward the message \(M\) to \(v_j\)
5: \(v_i\) will forward the message \(M\) to \(v_j\)
6: \(v_i\) will forward the message \(M\) to \(v_j\)
7: \(v_i\) will forward the message \(M\) to \(v_j\)
8: \(v_i\) will forward the message \(M\) to \(v_j\)
9: end if
10: end procedure

**Fig. 3.** Vehicle-to-RSU (V-2-I) communication

**Vehicle-to-RSU (V-2-I) communication:** Considering an average vehicle velocity of \(V = 60\) km/h \((\approx 16.6\) m/s) and a transmission range \(T_R = 300\) m, the communication interval \((\text{Cl})\) for the vehicle \(v_i\) and a stationary RSU located at intersection \(c_i\), as shown in Fig. 3, can be roughly calculated by \((\text{Cl}) = \frac{T_R}{V} = \frac{300}{60} = 5\) s. Note that, if there are traffic lights at the intersection, the CI can be longer than 36.1 s. Then, within the CI, the V-2-I communication is executed by the following steps:

- The RSU periodically broadcasts the beacon message within its coverage. Concretely, the RSU first chooses a random number \(a \in Z_q^*\) and computes the current timestamp \(T_j\) as \((\alpha_3, \beta_3)\), where
  \[ \alpha_3 = g^a, \beta_3 = a + x \cdot H(\alpha_3, T_j) \mod q \] (5)

  broadcasts the beacon information \((T_j, \alpha_3, \beta_3)\).
- After receiving the beacon message \((T_j, \alpha_3, \beta_3)\) at time \(T_j\), the vehicle \(v_i\) checks whether \(T_j - T_j \leq \Delta T\). If it doesn’t hold, \(v_i\) believes it is a replay attack and neglects it.
- Otherwise, \(v_i\) checks \(g^{\beta_3} = a \cdot C_j^{H(\alpha_3, T_j)}\) with the RSU’s public key \(C_j = g^b\). If it holds, the beacon message is accepted. The correctness and security can refer to [9].
- The vehicle \(v_i\) chooses a random number \(b \in Z_q^*\) to encrypt the destination location \(L_2\) as \(D = (\alpha_2, \beta_2) = (L_2 \cdot g^{gs y}, g^b)\) and sends \(M\) together with \(D\) to the RSU.
- Upon receiving \(M||D\), the RSU first recovers \(L_2\) from \(\alpha_2, \beta_2\) and chooses \(k_0, k_1 \in Z_q^*\) to re-encrypt the message \(M = (\alpha_0, \alpha_1, \beta_1, \beta_1)\) as
  \[ M = (\alpha_0, \alpha_1 k_0', \beta_0, \beta_1 k_1', \beta_1 k_1') = (m \cdot B_2^{k_0' + k_1}, g^{k_0 + k_1}, B_2^{k_1}, g^{k_1 k_1'}) \] (6)

Then, the RSU stores \(L_2||M\) and waits for the proper next-hop vehicle to carry it.

- Because the RSU is deployed at a high social intersection, the RSU may have already stored many messages. Therefore, if the vehicle \(v_i\) is willing to carry some of them to their destinations or other high social RSUs closer to their destinations, it will use the CPA technique \(\text{CPPA}(T_i||g^x)\) to again anonymously authenticate itself, where \(T_i\) is a new timestamp here. Then, after checking the validity of \(\text{CPPA}(T_i||g^x)\), the RSU, like the source node \(v_1\), will forward some messages to \(v_i\). We assume each message packet is 2 M and the packet transmission bitrate is 5 Mbps. (Note that, the 802.11p physical layer offers different bitrates, ranging from 3 to 27 Mbps, from which we can choose [10].) By deducing the cost around 2 seconds used for authentication between vehicle and RSU, we have \((\text{Cl} - 2)\cdot 5\) Mbps/2 M = \((36.1 - 2)\cdot 25\approx 85\). This result shows that almost 85 message packets can be forwarded between V-2-I communications.

**Vehicle-to-Vehicle (V-2-V) communication:** If no nearby RSU is found but an available vehicle \(v_j\) is passing by, then \(v_i\) will forward the message \(M\) to \(v_j\) with the V-2-V communications. The concrete interactive operations are same as those between \(v_1\) and \(v_i\) above. Consider both \(v_i\) and \(v_j\) having the same velocity \(V = 60\) km/h \((\approx 16.6\) m/s)
and transmission range $T_V = 300$ m, the communication interval (CI) between them on a straight road could become $CI = \frac{2 \cdot T_V}{2 \times 18.0} = 18.0$ s. This calculation indicates that forwarding between vehicle and vehicle should be fulfilled within 18.0 s. Because vehicle has no huge storage and is also not as social as RSU in our network model, then the 18-second CI can fit for fewer packet forwarding between V-2-V communications.

Packet dropping case: As show in Algorithm 1, if none of RSU or vehicle is found as an available next-hop node in vehicular DTN, the message $M$ has to be dropped.

Step 4. If the message $M = (\alpha_0, \beta_0, \alpha_1, \beta_1)$ is not dropped, it will eventually be relayed to the destination node $v_2$ at location $L_2$. Then, the destination node $v_2$ can use its secret key $x_2$ to recover $m$ by the following operations:

$$m_0 = \frac{\alpha_0}{\beta_0 \cdot \beta_2}, \quad m_1 = \frac{\alpha_1}{\beta_1 \cdot \beta_2}$$

If $m_0 \neq 1$ and $m_1 = 1$, the destination node accepts $m_0$ as the valid plaintext $m$; otherwise, the message $M = (\alpha_0, \beta_0, \alpha_1, \beta_1)$ is invalid and will be rejected.

Correctness. Suppose $M = (\alpha_0, \beta_0, \alpha_1, \beta_1)$ is temporarily stored at RSU only once, then it has the form of $(m \cdot B_2^{k_0 + k_1} k_0, B_2^{k_1} g_0^{k_0 + k_1} k_0, B_2^{k_1} g_1^{k_0} k_1)$. Thus,

$$\frac{\alpha_0}{\beta_0} = \frac{m \cdot B_2^{k_0 + k_1} k_0}{(g_0^{k_0 + k_1} k_0)^{2}} = m; \quad \frac{\alpha_1}{\beta_1} = \frac{B_2^{k_1} g_0^{k_0} k_1}{(g_1^{k_0} k_1)^{2}} = 1$$

If $M = (\alpha_0, \beta_0, \alpha_1, \beta_1)$ was stored in RSUs more than once, with simple deduction, the correctness on recovering the plaintext $m$ can also be checked. The details on this universal re-encryption technique can be referred to [8].

IV. SECURITY ANALYSIS

In this section, we analyze the security properties of the proposed SPRING protocol. In specific, following the threat model discussed earlier, our analysis will focus on how the proposed SPRING protocol can resist to the packet analysis attack, packet tracing attack, and the black (grey) hole attack, respectively.

A. Resilience to Packet Analysis Attack

In the proposed SPRING protocol, the source node $v_1$ has encrypted the sensitive message $m$ into $M = (\alpha_0, \beta_0, \alpha_1, \beta_1)$. Without knowing the destination node $v_2$‘s secret key $x_2$, the adversary can’t recover $m$ from packet analysis. In addition, because the CPPA anonymous authentication is adopted, no identity information will be disclosed. Therefore, the proposed SPRING protocol can resist the packet analysis attack.

B. Resilience to Packet Tracing Attack

First, we consider no vehicle nodes controlled by the adversary $A$ participate in the packet forwarding. Then, the capability of the adversary is limited to eavesdrop the interactions among V-2-V communications and V-2-I communications. Because the destination is encrypted in each interaction, the adversary can’t know the destination information. In addition, in the proposed SPRING protocol, when an RSU receives $M = (\alpha_0, \beta_0, \alpha_1, \beta_1)$ from a vehicle, it will use the universal re-encrypt technique to convert $M$ into another form $M = (\alpha_0 \cdot \alpha_1^{k_0}, \beta_0 \cdot \beta_1^{k_0}, \alpha_1^{k_1}, \beta_1^{k_1})$. Since $k_0$ and $k_1$ are randomly chosen from $\mathbb{Z}_n$, $(\alpha_0, \beta_0, \alpha_1, \beta_1)$ and $(\alpha_0 \cdot \alpha_1^{k_0}, \beta_0 \cdot \beta_1^{k_0}, \alpha_1^{k_1}, \beta_1^{k_1})$ are unlinkable. More importantly, since the RSU is located at a high social intersection, a large number of vehicles pass by and many packets will be temporarily stored at the RSU, the RSU can naturally serve as a mix server, as shown in Fig. 4. Then, for a specific message packet, only if it had been temporally stored in a high social RSU at least once, the adversary can’t trace it only by eavesdropping.

Fig. 4. High social RSU serves as a mix server in vehicular DTN

Second, we consider some vehicles controlled by the adversary $A$ participate in the packet forwarding. Clearly, in this case, the destination information is disclosed to the adversary. However, in the proposed SPRING protocol, 1) the source node $v_1$ is indistinguishable from other intermediate nodes during the V-2-V and V-2-I communications; 2) the real identity won’t be disclosed in the CPPA anonymous authentication, the adversary still can’t determine who is the indeed source node. By summarizing the above, the proposed SPRING protocol can resist the packet tracing attack.

C. Resilience to Black (Grey) Hole Attack

Because of the CPPA anonymous authentication, the black (grey) attacks launched by the external adversary can be efficiently resisted in the proposed SPRING protocol. However, once the vehicle nodes controlled by the adversary $A$ launch the black (grey) attacks, because they know the valid key materials, and at the same time, the CPPA anonymous authentication also makes them unlinkable, the black (grey) attacks in this case are serious and hard to resist. Fortunately, the privacy preservation provided by the CPPA technique is conditional, which provides the second line of defense. Once the witness CPPA$(T_i || g^x)$ is submitted to the TA, the TA can reveal the real identity by using the conditional tracking algorithm in Section III-A. Thus, if a message packet doesn’t reach the destination $L_2$, then with the chain tracking policy shown in Fig. 5, each next-hop node participating in such packet’s forwarding can be identified by the TA with the witness CPPA$(T_i || g^x) || L_2$ provided by the current node, where the destination $L_2$ is used to assist the current node to identify the involved next-hop node among many next-hop nodes. If the current node can’t provide any witness, it becomes suspicious.
Fig. 5. Detect the suspicious vehicle nodes with chain tracking

As shown in Algorithm 1, if no next-hop node is available, the message packet can also 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 the detection process in Algorithm 2, the vehicle nodes who launched the black (grey) hole attacks can be identified. Note that, in the Algorithm 2, the thresholds $T_B$, $T_G$ must be carefully defined. Otherwise, false positive and false negative could be high.

Algorithm 2 Detection of black (grey) hole attacks
1: procedure BLACKGREYHOLEATTACKDETECTION
2: With the chain tracking in Fig. 5, the TA can obtain each vehicle node $v_i$’s packet dropping number, denoted as $X_i$.
3: Compute the mean $X$ of all vehicle nodes $V = \{v_1, v_2, \cdots\}$ as $X = \frac{1}{|V|} \sum_{i=1}^{|V|} X_i$, where $|V|$ is the cardinality of $V$.
4: Compute the distance of each $X_i$ to the mean $X$ as $d(X_i) = |X_i - X|$.
5: Define the thresholds $T_B$, $T_G$ for black hole attack and grey hole attack, respectively.
6: for each vehicle node $v_i \in V = \{v_1, v_2, \cdots\}$ do
7: if $d(X_i) > T_B$ then
8: $v_i$ is considered as a black hole attacker.
9: else if $d(X_i) > T_G$ then
10: $v_i$ is considered as a grey hole attacker.
11: else
12: $v_i$ is considered as a normal vehicle node.
13: end if
14: end for
15: end procedure

V. PERFORMANCE EVALUATION

In this section, we study the average-case performance of the proposed SPRING protocol, using a custom simulator built in Java. The performance metrics used in the evaluation are average delivery ratio (DR) and packet average delay (AD), where the DR is defined as the average ratio of the packets successfully delivered to the destinations with respect to those generated by the sources within a given time period, and the AD is defined as the average time between when a packet is generated at some source and when it is successfully delivered to the destination. In addition, following the earlier design goal, we also evaluate the resistance to packet tracing attack and detection of black (grey) hole attacks in the simulations.

A. Simulation Setup

To simulate a sparse vehicular DTN, 50 vehicle nodes with transmission radius of 300 meters are first deployed to cover an interest Kitchener-Waterloo (K-W) region of 6,000 m × 15,000 m, as shown in Fig. 6. In addition, 12 intersections are chosen as the candidates for RSU deployment in the region.

![Fig. 6. Kitchener-Waterloo (K-W) region considered for simulation](image)

Mobility model. In vehicular DTN, the performance of packet forwarding is highly contingent upon the mobility of the vehicle nodes. Because the vehicle nodes are mostly driven by the citizens, modeling the mobility patterns of citizens in a specific area (i.e., K-W region) can achieve a relatively accurate performance evaluation. Let $s_0$ denote the state that a person is located at any spot in the K-W region, and state $s_1$, where $s_1 \subset s_0$, denote the person is stationary at some spot in the downtown. A person stays at each state $s_i$, $i \in \{0, 1\}$, for $120 \pm 60$ seconds, and then chooses the next state. If the current state is $s_0$, s/he will choose $s_1$ as the next state with the probability $\rho = 0.5$ and $s_0$ with the probability $1 - \rho$. If the current state is $s_1$, s/he will choose $s_0$ with the probability 1. Once the next state is determined, the person will drive the vehicle to the destination by following the map-based shortest path routing with the velocity 60 km/h.

![Fig. 7. Selection of high social intersections](image)

High-social intersection selection & RSU deployment. Because each vehicle node follows the map-based shortest path routing, we can use the simulations to statistically test the social degree of each intersection in Fig. 6. Based on the definition of social degree in EQ. (2), the duration for each simulation is set as one hour — a unit of time, and the results, as shown in Fig. 7, are averaged over 1,000 runs. After setting a proper social threshold (ST), we can select high-social intersections $HS = \{c_5, c_6, c_7, c_8\}$, and place an RSU at each intersection $c_i \in HS$. To examine the outstanding performance of social-based RSU deployment in the proposed SPRING protocol, we compare it with random RSU deployment, complete RSU deployment and non RSU deployment in vehicular DTN. The detailed parameter settings are summarized in Table I.
In the following, we conduct the simulations with different parameter $T_h$ and different RSU deployment. For each case, we run the simulation for 10 hours, and the average performance results over 20 runs are reported.

![Graphs showing delivery ratio and average delay for different time periods.](image)

**B. Simulation Results**

1) Delivery Ratio & Average Delay: Fig. 8 shows the delivery ratio varies with the specified period from 1 hour to 10 hours. From the figure, we can see the delivery ratio in group 1 is lower than that in groups 2, 3 and 4. This observation validates that the V-2-V plus V-2-I based forwarding is more reliable than the pure V-2-V based forwarding in vehicular DTN. Comparing the delivery ratio in groups 2, 3 and 4, we can also observe that the more the RSUs are deployed, the higher the deliver ratio; when the number of deployed RSUs are constrained, the social-based RSU deployment can achieve better deliver ratio than the random RSU deployment. In addition, Fig. 8 also shows that, when the parameter $T_h$ increases, a vehicle node has more chances to contact next-hop DTN nodes (vehicle and RSU), and the delivery ratio will visibly increase.

![Graph showing average delay for different time periods.](image)

2) Free Packets from Tracing Attack: As we mentioned earlier in Section IV, the RSUs naturally serve as Mix servers in the proposed SPRING protocol. Once a packet was temporarily stored at least in one RSU, it can resist the packet tracing attack launched by the external adversary. Fig. 10 shows the average number of successfully delivered packets in different RSU deployments. From the figure, we can observe, the more the RSUs are deployed, the more the successfully delivered packets and the more the packets that are temporarily stored at least in one RSU, as a consequence, the more packets can get rid of the packet tracing attack. Further observing the results in groups 2 and 3, we can conclude that the social-based RSU deployment can achieve better effects than the random RSU deployment in the proposed SPRING protocol.

3) Detection of Black (Grey) Hole Attacks: The proposed SPRING protocol provides the second line of defense to detect black (grey) hole attacks in privacy-preserving forwarding in vehicular DTNs. To evaluate the detection effect, we consider 5 black hole attackers and 5 grey hole attackers (with packet dropping probability ($PDP=50\%$) among the total 50 vehicle nodes in the simulations. Then, Fig. 11 depicts the detection effects in different groups. From the figure, we can see, i) when...
Therefore, when we choose proper thresholds more RSUs are deployed, the average dropped events will decrease; ii) the social-based RSU deployment has low average dropped events than that in the random RSU deployment. Therefore, when we choose proper thresholds $T_B$ and $T_G$ in Algorithm 2, these black (grey) hole attackers can be detected. Note that, because the grey hold attackers selectively drop the packets, the threshold $T_G$ should be more carefully chosen than $T_B$, especially when the PDP is low in grey hold attacks.

VI. RELATED WORK

Recently, two research works on packet forwarding in DTNs are appeared, which are closely related to the proposed SPRING protocol [4], [11]. In [4], Banerjee et al. perform an experimental and analytical study of mobile networks enhanced with relays, meshes, and wired base stations. In specific, the authors first deploy a large-scale vehicular network and use wired base stations, meshes and relay nodes as the stationary nodes deployed in an interesting area to temporarily store packets for delivery to other mobile nodes, propagating information towards the final destination. This work has the same idea on “stationary node’s assistance” as the proposed SPRING protocol. However, the security and privacy preservation issues are not addressed in the work.

In [11], Hui et al. show that it is possible to detect characteristic properties of social grouping in a decentralized fashion from a diverse set of real world traces, and demonstrate that such characteristics can be effectively applied in packet forwarding decisions in DTN. Concretely, based on the observations that human interaction is heterogeneous both in terms of popular individuals and groups or communities, Hui et al. propose a social based forwarding algorithm (BUBBLE) for pocket switched networks (PSNs). The experimental results show that the BUBBLE algorithm can significantly improve the forwarding efficiency. Nevertheless, the security and privacy preservation issues are still not discussed in BUBBLE.

Distinct from the above works, the proposed SPRING protocol not only heuristically studies the social-based RSU deployment for enhancing the delivery ratio in vehicular DTNs, but also discusses the privacy preservation issues as well as black (grey) hole attacks in vehicular DTNs.

VII. CONCLUSIONS

In this paper, we have presented a social-based privacy-preserving packet forwarding (SPRING) protocol for vehicular DTNs. Based on social-based RSU deployment, the proposed SPRING protocol has been identified to be not only capable of significantly improving the reliability with V-2-V and V-2-I communications, but also able to achieve the privacy preservation and resist the black (grey) hole attacks in packet forwarding. Through extensive performance evaluation, we have demonstrated that the proposed SPRING protocol can achieve much better efficiency in terms of delivery ratio in vehicular DTNs.

REFERENCES