On Secure VANET-Based Ad Dissemination With Pragmatic Cost and Effect Control

Zhengming Li, Congyi Liu, and Chunxiao Chigan

***Abstract*—Allowing commercial service providers (SPs) to promote their businesses, ad dissemination in vehicular ad hoc networks (VANETs) shows great application potential. In this paper, a VANET-based Ambient Ad-Dissemination scheme (VAAD) is proposed to support secure ad disseminations with pragmatic cost and effect control. VAAD provides an incentive-centered architecture for the involved parties to trade off their conflicting requirements regarding ad dissemination. Given realistic advertising effect and cost requirements of an SP, VAAD adopts a distance-based gradient ad dissemination algorithm to maximize the achievable ad effect by emulating the ad-posting patterns in the physical world. To facilitate vehicular nodes' participation in VAAD, efficient, secure, and privacy-preserving incentive cash-in is ensured to support financial transactions in VAAD. Thus, with proper cost and effect control, VAAD is a novel and comprehensive solution to secure ad dissemination in VANETs.**

***Index Terms*—Ad dissemination, privacy, security, vehicular ad hoc networks (VANETs).**

I. Introduction

VEHICULAR ad hoc networks (VANETs) promise great enhancement to traffic safety and traffic management [1], [2] with wireless vehicle-to-vehicle and vehicle-to-roadside communications. Specifically, enabling nearby vehicles to wirelessly share driving states, VANETs enable various traffic safety applications such as collision avoidance and lane change assistance. In addition, in VANETs, real-time traffic data can be collected from vehicles to improve traffic management. Thus, the potential to improve traffic safety and traffic management will push VANETs to be massively deployed in the future. Furthermore, with free vehicular communications, VANETs provide a handy platform to more cost effective solutions to various value-added applications, e.g., on-road entertainment [3] and automatic survey [4]. Comparatively, existing cellular communications [third-generation (3G) and fourth-generation (4G)] will incur service fees to support such value-added applications.

Considering numerous vehicles available in VANETs, one particularly attractive value-added application is for commercial service providers (SPs) to promote their businesses with VANET-based ad dissemination. In addition to being more cost effective than ad dissemination based on cellular communications, VANET-based ad dissemination can easily target ad receivers in specific regions. On the other hand, VANET-based ad dissemination is more cost effective and flexible than roadside ad posters, which involve costly human efforts in ad posting and update.

However, without pragmatic cost and effect control, arbitrary ad disseminations from various SPs may cause unnecessary distractions to drivers and message storms to VANETs. In addition, the security and privacy issues of ad dissemination also call for thorough investigation.

As further discussed in Section II, the existing schemes only, at best, partially tackle the aforementioned challenges. Thus, in this paper, a VANET-based Ambient Ad-Dissemination scheme (VAAD) is proposed to ensure secure ad dissemination with pragmatic cost and effect control. Specifically, VAAD features three major contributions.

1) An incentive-centered architecture is proposed to encourage the SPs to set reasonable cost and effect requirements for ad dissemination.
2) A novel distance-based gradient (DBG) algorithm is proposed to disseminate ads to emulate the ad posting patterns in the physical world and control the cost and effect of ad dissemination.
3) An efficient, secure, and privacy-preserving incentive cash-in algorithm is proposed to encourage the cooperation of vehicular nodes and support economic value creation.

The rest of this paper is organized as follows: Section II reviews the related work. Section III presents the background and architecture of VAAD. The detailed algorithms of VAAD are presented in Sections IV and V. Discussions on VAAD's application potentials are presented in Section VI, followed by detailed analysis and simulations of VAAD's performance in Section VII. Section VIII concludes this paper.

II. Related Work

In VANETs, information of various services can be broadcasted (*pushed*) to the targeted vehicular nodes or be queried (*pulled*) by interested nodes. The representative schemes based on the pull model [5]–[8] allow each node to query and discover the available services in an interested region. Comparatively, the push model-based approach allows SPs to proactively advertise their services to a broader range of receivers, which is our major focus in this paper.

Focusing on routing performance, the existing routing schemes [9]–[14] pay no attention to messages' application

Manuscript received September 23, 2011; revised March 16, 2012 and May 21, 2012; accepted June 19, 2012. Date of publication July 19, 2012; date of current version February 25, 2013. This work was supported by the National Science Foundation CAREER Award under Grant CNS-0644056. The Associate Editor for this paper was G. Yan.

The authors are with the Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, MI 49931 USA (e-mail: zli1@mtu.edu; congyil@mtu.edu; cchigan@ieee.org).

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.2012.2206111

relevance. Thus, such schemes may not be directly adopted for ad dissemination in VANETs since they may lead to a harmful broadcast storm in the face of numerous ads.

Several schemes considering message context/content in general message dissemination have also been proposed. For instance, [15] introduces the enhanced distributed channel access mechanism based on IEEE 802.11e for the high-loaded scenarios. In [16], strategies for context-adaptive message dissemination were proposed with several metrics to estimate the benefits of local danger warning messages to the receivers. Similarly, [17] also allows each node to estimate the application relevance of its buffered messages and schedule the message transmissions accordingly. A message dissemination paradigm is proposed in [18] to allow each roadside unit (RSU) to encode a huge message into k data packets with rateless coding, which may be adopted in the dissemination of multimedia ads. In [19], AdTorrent implements a push-model-based location-aware distributed mechanism to search, rank, and deliver relevant ads. However, the aforementioned schemes generally ignore critical security and privacy issues, as well as cost and effect control of ad dissemination.

To our best knowledge, Signature-Seeking Drive (SSD) [20] is most relevant to our work, proposing incentive-based ad dissemination for VANETs. SSD designs level-free, one-level, and n-level ad-dissemination models to reward ad forwarders based on the receipts generated by ad receivers, which can encourage vehicular nodes to willingly participate in ad dissemination. However, in SSD, the advertising effect cannot be measured or controlled since the number of collected receipts cannot precisely reflect the number of actual ad receivers. Indeed, except for the one-level dissemination model, the geographic range of ad dissemination cannot be controlled in SSD, which ignores the ads' location relevance. In addition, in SSD, each ad receiver who generates receipts will also be rewarded with incentive, which is somewhat inconsistent to the general real-world advertising model.

Comparatively, VAAD provides a more realistic incentive-based ad dissemination model with pragmatic cost and effect control. In addition, the critical security and privacy issues in ad dissemination are carefully considered in VAAD.

III. Background and System Architecture

In this section, the background and system architecture of VAAD are presented. For clarity, the common notations used throughout this paper are listed in Table I.

TABLE I
COMMON SYMBOLS

Symbol	Meaning
PR_X	The private key of an entity X
PU_X	The public key of an entity X
$Cert_X$	The certificate of an entity X
$Key\{Msg\}$	A message Msg encrypted with Key
$\{Msg\}PR_X$	Digital signature of Msg signed with PR_X
p	Decreasing gradient of ad density
L	Length of the unit road segment
D_i	Requested distance of the ith ad rebroadcast
R	Common communication range of vehicular nodes
D_D	Desired ad dissemination distance specified by a SP
$(N_{FT})N_F$	(Theoretic) Number of ad forwarders in an ad rebroadcast
$(N_{RT})N_R$	(Theoretic) Number of ad receivers in one ad rebroadcast

A. Network Model and Assumptions

Based on common assumptions [21], [22], in VANETs, vehicular nodes equipped with Dedicated Short-Range Communication (DSRC) [23] devices form the *ad hoc domain*. Each node periodically (with a period from 100 to 500 ms) broadcasts beacons containing the driving states, such as location, speed, and heading direction, to support traffic safety applications. Each node is equipped with multiple pseudonyms to protect its privacy with pseudonym changes [2], [24]–[26]. For security, each node needs to digitally sign its data packets with a valid private key, as issued by the VANET Authority. A tamper-proof device [27] in each node keeps its pseudonyms confidential and prevents it from launching Sybil attack [28] by allowing the use of only one pseudonym at any time. Most vehicular nodes are assumed to be rational (honest and selfish): being selfish, one node can be encouraged to participate in VAAD with incentives; being honest, one node will comply with the application protocols once it agrees to participate in VAAD.

In the *infrastructure domain* of VANETs, the *Authority* is in charge of the management functions, such as certificate issuing, reputation management, and security provisioning. In addition, a *clearance center* (CC) supports the financial transactions in VANETs. As access points to the infrastructure domain, the RSUs are sparsely deployed in VANETs due to cost considerations. All infrastructure entities are trustworthy regarding their functions.

B. Ad Dissemination Model

In this paper, an *SP* refers to a business entity with a fixed position, such as a restaurant or a gas station. We leave mobile SPs, such as vehicles that are willing to share music, to service discovery schemes [5]–[8]. To impress more customers, an SP may disseminate one ad multiple times with a certain frequency, where each is denoted as an *ad rebroadcast*.

Due to the location relevance of most ads in VANETs, the SP will request one specific RSU[1] (usually the RSU nearest to itself) to act as its *source RSU (SRSU)* and broadcast its ad to the nearby vehicles. To cover a larger area than the communication range of the SRSU, the ad needs to be forwarded by vehicular nodes over multiple hops.

Therefore, ad dissemination involves three parties with conflicting requirements: First, each SP intends to maximize its advertising effect by disseminating ads to as many nodes as possible. Second, as an ad receiver, each node would like to learn of the local services without being distracted by excessive ads. In addition, being selfish, each node forwarding one ad expects to receive certain incentive in return. Third, VANETs as a whole need to ensure ad dissemination is under control in the face of increasingly more ads to avoid message storms.

[1]In reality, one SP may choose to disseminate its ad to multiple regions via multiple SRSUs. Generally, such regions should not overlap to maximize advertising effect with a limited cost budget. Thus, in this paper, we focus our efforts on one SRSU for each SP.

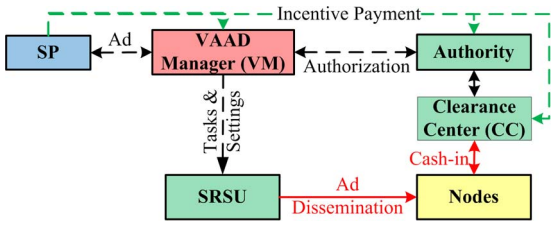


Fig. 1. Overview of VAAD.

Meantime, the infrastructure entities may also expect to obtain incentives for supporting ad disseminations. All these conflicting requirements need to be balanced in VAAD.

C. VAAD Architecture

As shown in Fig. 1, VAAD is proposed to support secure ad dissemination with pragmatic cost and effect control. To trade off the conflicting requirements of the involved parties, an incentive-centered architecture is proposed for VAAD, where the SP pays other entities for their services in ad dissemination. Constrained by the incurred cost, each SP will set a realistic advertising effect requirement in terms of the number of ad receivers and the ad rebroadcast frequency. The VAAD Manager (VM) is introduced to coordinate the interactions between SPs and VANETs. Upon receiving a dissemination request from one SP with cost and effect specifications, the VM will obtain proper authorization from VANET Authority for this ad. With the authorization, the VM can request one SRSU to disseminate the ad according to the specifications. For brevity, the registration and authorization procedures of VAAD are omitted here. Our previous value-added applications [4], [29] provide useful reference to this end.

Within this incentive-centered system architecture, two novel algorithms are proposed to support pragmatic cost and effect control for secure ad dissemination in VAAD.

DBG Ad Dissemination: Inspired by the ad posting pattern in the physical world, a DBG ad-dissemination algorithm is proposed in VAAD to maximize the advertising effects, given a cost budget. With this algorithm, the ads will be disseminated in such a way that the ad packets form a virtual ad poster in VANETs. When vehicles drive around, they will receive ad packets about local services as if they were driving by real ad posters in the physical world. That is, the closer one vehicle is to an SP, the more frequently it will receive the ads from this SP. As such, the location relevance of ads is exploited to increase the actual advertising effect, given a realistic cost budget.

Cash-In: To encourage vehicular nodes to strictly follow the ad dissemination requirements, certain incentive will be rewarded to each ad forwarder. A novel cash-in algorithm is designed to ensure that each ad forwarder can securely and indisputably prove its ad forwarding services and obtain its deserved incentive from the CC in a privacy-preserving way.

D. Adversary Model

In VAAD, an SP may repudiate any liability related to its previously disseminated ad or forge false ads in the name of its competitors. The malicious vehicular nodes may attempt to gain undue personal interests or sabotage VAAD by forging, playing back or/and tampering with ads, or claiming ads that they have not forwarded. Meanwhile, the SPs, CC, and RSUs may attempt to derive personal information about vehicular nodes in VAAD, which will potentially harm vehicles' privacy.

All these attacks need to be properly handled to ensure the proper functioning of VAAD and make VAAD widely accepted by the privacy-sensitive users.

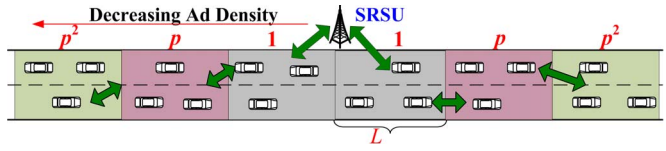


Fig. 2. Ad density gradient in highway scenario.

IV. Distance-Based Gradient Ad Dissemination

In VANETs, the relevance of an ad mainly depends on the distance from the ad receiver to the SP. For instance, in downtown areas, the ad of a parking lot is more relevant to the drivers 1 km away than to those 10 km away. In highway scenarios, the ad of a gas station is also more relevant to the nearby drivers. By exploiting such location relevance, a novel DBG ad dissemination algorithm is proposed to maximize the effect of ad dissemination given a limited cost budget.

A. DBG: Propagation Model

The DBG attenuates the density of a particular ad with a *gradient* $p \in [0, 1)$ as the distance increases by a unit road segment L from the SRSU, as shown in Fig. 2. Thus, the DBG forms virtual roadside ad posters around the SRSU, which will notify the upcoming vehicles of local services with increasing intensity as the vehicles get closer. As such, the location relevance of ads is fully exploited by DBG. By properly configuring p and L, as discussed in Section VII-A, each SP can achieve its desirable cost and effect for ad dissemination.

To achieve the desirable ad density gradient in Fig. 2, the SRSU sets the requested dissemination distance D_i for each ad rebroadcast by selecting D_i with the probability

$$Pr\{D_i = kL\} = (1-p)p^{k-1}, \qquad k = 1, 2, \ldots \tag{1}$$

In both 1-D (highway) and 2-D (downtown) scenarios, D_i indicates the requested ad dissemination distance from the SRSU. With D_i determined by (1), over a long period, the ad density gradient is p in both 1-D and 2-D scenarios. Specifically, in 1-D scenarios, number the road segments from the SRSU as 0, 1, and so on. Thus, an ad will reach the jth road segment with probability

$$\begin{aligned} Pr\{D_i \geq (j+1)L\} &= 1 - Pr\{D_i \leq jL\} \\ &= 1 - \left[(1-p) + (1-p)p + \cdots + (1-p)p^{j-1}\right] \\ &= p^j. \end{aligned}$$

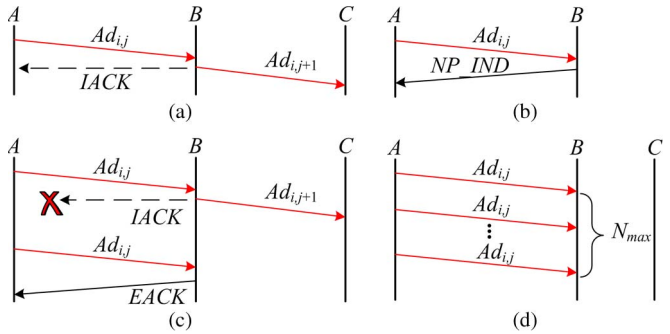


Fig. 3. Possible cases in ARQ-based ad forwarding.

Thus, over a long period, the decreasing gradient is p. The proof for 2-D scenarios is similar.

To encourage vehicular nodes to forward the ad according to D_i, VAAD will give incentives only to the ad forwarders within distance D_i from the SRSU based on the geographic information contained in the ad packets. Thus, vehicles within D_i from the SRSU are economically encouraged to forward the ad, and the vehicles outside D_i have no incentive to forward the ad further. Hence, by properly configuring p and L, the DBG will control ad dissemination with the desired ad-dissemination cost and effect specified by the SP, as verified in Section VII-A.

B. Reliable and Efficient Ad Forwarding

To be cost effective, in VAAD, it is necessary to minimize the number of ad forwarders while ensuring reliable ad forwarding within distance D_i from the SRSU. To this end, reliable and efficient ad dissemination procedures in each hop are proposed, which includes *road segment mode, intersection mode*, and *border mode*. Here, it is reasonably assumed that, with GPS devices and periodical beacons [23], each node knows its location and the locations of its one-hop neighbors.

Road Segment Mode: ARQ-Based Ad Forwarding: Within each road segment, the current ad forwarder (e.g., node A) needs to select a proper downstream ad forwarder out of its one-hop neighbors to ensure reliable and efficient ad forwarding. To this end, A first estimates the *average forwarding distance* of each neighbor, e.g., B, as follows:

$$\bar{d}_{AB} = d_{AB}/(1/Pr_{AB}) = Pr_{AB} \times d_{AB}. \tag{2}$$

Here, Pr_{AB} is the probability that node B will successfully receive the data packet from node A, estimated based on the channel attenuation and fading models [30] of vehicular wireless communications. d_{AB} indicates the distance between A and B. As shown in (2), to send one ad packet to B, on average, A needs $1/Pr_{AB}$ transmissions, so $\bar{d}_{AB}$ indicates the expected efficiency of ad forwarding between A and B.

Hence, A will first select the neighbor with the highest average forwarding distance, e.g., B, as the next ad forwarder. In case of a tie, A will randomly select one neighbor with the highest average forwarding distance. An Automatic Repeat reQuest (ARQ)-based algorithm [31] is proposed to ensure reliable ad forwarding between A and B, as shown in Fig. 3, which consists of four cases, as discussed here.

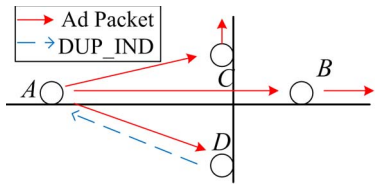


Fig. 4. Ad propagation in intersection mode.

Successful Forwarding With IACK: As shown in Fig. 3(a), A first sends its ad packet $Ad_{i,j}$ (ith ad rebroadcast at jth hop) to B. Upon receiving $Ad_{i,j}$, B will similarly select its downstream ad forwarder C and send the ad packet as $Ad_{i,j+1}$ to C. Due to the nature of wireless communication, A overhears $Ad_{i,j+1}$ and regards it as an implicit ACK (*IACK*) from B. Thus, A is sure that B has successfully received $Ad_{i,j}$ and forwarded it.

Successful Forwarding With EACK: As shown in Fig. 3(b), A first sends $Ad_{i,j}$ to B, and B also forwards it to C. However, due to possible medium-access control layer collisions, A fails to overhear $Ad_{i,j+1}$. Thus, after a preset period, A will retransmit $Ad_{i,j}$ to B. Upon receiving the second $Ad_{i,j}$, B will send $Ad_{i,j+1}$ as an explicit ACK (*EACK*) to A to indicate that it has already forwarded $Ad_{i,j+1}$.

Network Partition: As shown in Fig. 3(c), B may face a network partition and cannot forward the ad further. In this case, B will send an network partition indication (*NP_IND*) message to A to indicate the presence of a network partition so that A will not try to retransmit the ad to B.

Unsuccessful Forwarding: As shown in Fig. 3(d), A has retransmitted $Ad_{i,j}$ for a preset retransmission threshold $N_{\max}$ without receiving *IACK*, *EACK*, or *NP_IND* from B. In this case, A will assume that B is unable to forward the ad packet, and select the next best neighbor as the new downstream ad forwarder to repeat the preceding procedures.

The optimal $N_{\max}$ for A in sending the ad to B can be configured based on Pr_{AB} as

$$N_{\max} = \lceil 2/Pr_{AB} \rceil. \tag{3}$$

Equation (3) ensures that, with high probability, A will successfully send its ad to B (through $1/Pr_{AB}$ transmissions) and would receive B's response (through $1/Pr_{AB}$ transmissions) if B is willing to cooperate. In addition, SPs can determine the proper incentive for the ads, so that most vehicular nodes will be willing to cooperate in VAAD. As such, reliable and efficient ad forwarding can be ensured in each hop.

Intersection Mode: In VANETs, each node can figure out whether it is nearby or in a road intersection, either with a preloaded digital map or based on the location distributions of its neighbors. Here, a road intersection could be an intersection formed by several single-lane or multiple-lane road segments. For brevity, here, we use a typical four-road intersection as an example.

If the current ad forwarder A is nearby or in a road intersection, it will enter the *intersection mode* and select the best downstream node with (2) on each road segment running away from the SRSU, e.g., B, C, and D, as shown in Fig. 4. Then,

A will send the ad packet to each of these nodes, following the same procedures as the road segment mode. Here, for simplicity, we omit the signal blocking effects of the buildings around the intersection.

To avoid duplicate ad forwarding, if one node D has already received the same ad packet from another node, it will send this ad packet as a duplicate ad indicator (*DUP_IND*) to A to indicate that this road segment has already been covered by the concerned ad. Thus, A will stop sending the ad packet to the road segment of D.

Following the aforementioned procedures, the intersection mode can ensure full coverage of the desired ad dissemination area without duplicate ad packets.

Border mode: An ad forwarder (e.g., node A) is on the border of the propagation region if its distance to the SRSU is between $D_i - R$ and D_i. In this case, A enters the *border mode* by broadcasting the ad packet without selecting the next forwarder. Thus, any node overhearing the ad packet generally will not forward it due to the lack of incentives. As such, the ad dissemination region will be controlled to be D_i, resulting in a certain number of ad forwarders to be rewarded with incentives.

C. Secure Packet Format

To support secure ad forwarding, the ad packet forwarded by each node *A* has the following secure format:

$$P_A = \{Payload = \{ID_{\mathrm{AD}}, SeqNum, Loc_A, TSP_A, ID_{\mathrm{PRE}}, ID_A, \{ID_{\mathrm{NEXT}}\}, DATA_{\mathrm{AD}}\}, \{Hash(Payload)\}\, PR_A, Cert_A\}.$$

Here, ID_{AD} is the identifier of this ad. $SeqNum$ is the sequence number of the current ad rebroadcast. Loc_A and TSP_A are the current location and timestamp of node A, respectively. ID_A is the pseudonym of node A. ID_{PRE} and ID_{NEXT} indicate the upstream and downstream ad forwarders, respectively. As discussed in Section IV-B, in 2-D scenarios, there may exist multiple downstream ad forwarders in each hop. $\{Hash(Payload)\}PR_A$ is A's digital signature for the hash value of $Payload$. $Cert_A$ is A's certificate issued by the Authority, as shown in Table I. $DATA_{\mathrm{AD}}$ is given as

$$DATA_{\mathrm{AD}} = \{Data = \{ID_{\mathrm{SP}}, TSP_{\mathrm{SP}}, ID_{\mathrm{SRSU}}, Loc_{\mathrm{SRSU}}, D_i, Incentive, Content\}, \{Hash(Data)\}\, PR_{\mathrm{SRSU}}, Cert_{\mathrm{SRSU}}\}.$$

$DATA_{\mathrm{AD}}$ is created by the SRSU to contain the ad content $(Content)$ and the requested dissemination distance D_i for each ad rebroadcast, based on SP's requirements. Here, ID_{SP} is the ID of the source SP. ID_{SRSU} and Loc_{SRSU} are the ID and the location of the SRSU, respectively. $Incentive$ indicates the incentive for each ad forwarder.

At each hop, the ad forwarder is expected to update Loc_A, TSP_A, and the ad forwarder IDs and sign this packet with its private key. In case that one ad forwarder tampers with other data fields in the ad packet, its neighbors can detect this tampering with overhearing. Each ad receiver can verify the integrity of this ad packet based on the digital signature. Thus, with this, secure packet format message authenticity and integrity can be ensured. In addition, as discussed in Section IV-B, this packet can also serve as *EACK* and *DUP_IND* when necessary.

In addition, the *NP_IND* message generated by a node, e.g., B, has the following format:

$$NP\_IND = \{Payload = \{ID_B, NP, Loc_B, TSP_B\}, \{Hash(Payload)\}\, PR_B, Cert_B\}.$$

Here, NP indicates the type of this message. With this message format, node B cannot repudiate the *NP_IND* it sent out. Thus, if B wrongly sends out a *NP_IND* message when it is still surrounded with multiple neighbors, its neighbors can detect this false *NP_IND* and punish B's misbehaviors as in [32]. Here, for brevity, we assume that any nodes only send out valid *NP_IND* messages.

V. Secure and Privacy-Preserving Cash-In

In VAAD, it is critical to enable ad forwarders to get their deserved incentives from the SP with the help of the CC. Here, we assume that the SP has already paid the CC in advance so that the CC will handle the cash-in request of the ad forwarders. However, in VANETs, with privacy protection (enabled by changing pseudonyms [24]–[26], [33]), this cash-in process is challenging in several ways: First, it is difficult to verify the ad forwarders since a node may forge ad forwarding proof with its multiple pseudonyms. Second, due to the time delay between ad forwarding and cash-in, one ad forwarder may assume a different pseudonym in cash-in than the pseudonym used in ad forwarding. The connection between these two pseudonyms should be kept secret from both SP and CC, which is a basic requirement for privacy protection in VANETs [24]–[26], [33]. Third, due to privacy protection, the location of each node at any time is unknown to the SP or CC, which makes it difficult to distribute the incentive to each ad forwarder.

To address these challenges, a secure and privacy-preserving cash-in algorithm is proposed in this section.

A. Main Idea

The cash-in algorithm consists of two components: 1) ad forwarder verification and 2) incentive distribution. Specifically, after forwarding an ad, each ad forwarder will construct a proof of forwarding (*PF*) and send it to the CC via the next available RSU. The CC collects the PFs regarding one ad rebroadcast for a reasonably long time period, which can be determined based on the node mobility and RSU density in VANETs. After that, the CC will verify the ad forwarders by constructing an ad forwarding chain for this ad. In this process, one malicious node may attempt to forge a proof for an ad it did not forward, or it may intentionally refuse to submit its valid proof to disrupt the CC. Additionally, one node may fail to submit its valid proof due to communication failures. Moreover, several malicious nodes may collude to vouch for one another to cheat the CC into accepting their invalid proofs. Hence, a PF and

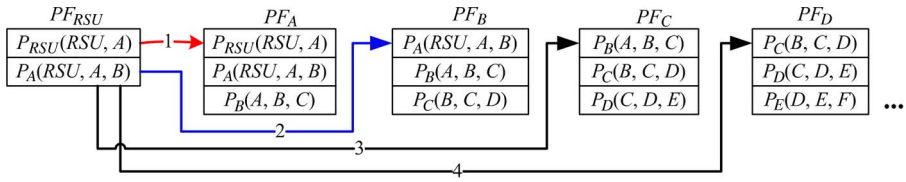


Fig. 5. Various cases in identifying the next ad forwarder.

the ad-forwarding chain will be designed to ensure secure and reliable ad forwarder verifications by detecting and handling these attacks.

The CC will then encrypt the incentive for each verified ad forwarder and publish them in a website where each ad forwarder can confidentially query its incentive.

B. Secure and Reliable Ad Forwarder Verification

To enable each ad forwarder to indisputably prove its ad forwarding service to CC, an *unforgeable PF* format is proposed here. Each ad forwarder, e.g., node B, will construct its PF as follows:

$$PF_B = \left\{ Proof = \left\{ SK_B \left\{ P_A^-, P_B^-, P_C^- \right\}, PU_{\mathrm{CC}} \{SKB\} \right\}, \right. \\ \left. \{Hash(Proof)\} PR_B, Cert_B \right\}.$$

Here, A and C denote the upstream and downstream ad forwarders of B, respectively, as shown in Fig. 5. P_A^-, P_B^-, and P_C^- are the ad packets forwarded by A, B, and C, respectively, excluding $DATA_{\mathrm{AD}}$ (see Section IV-C). SK_B is a secret key established by B to be shared with the CC. The embedded ad packets are encrypted with SK_B, and SK_B itself is encrypted with the public key of CC, i.e., PU_{CC}.

Furthermore, the pseudonym of B in PF_B should be the same as the ad forwarder ID in P_B^-. Thus, only B itself is able to construct a valid PF_B, and any single malicious node cannot forge a PF for an ad it has not forwarded. In addition, to prevent misbehaving nodes from colluding in forging PFs, the CC will construct an ad-forwarding chain based on collected PFs.

Specifically, after collecting PFs for a preset period, the CC will complete the embedded ad packets in each PF with the common $DATA_{\mathrm{AD}}$ field and make their digital signatures verifiable. Here, we denote the consecutive downstream ad forwarders of $SRSU$ as A, B, C, D, E, etc. The PFs from these ad forwarder nodes with their embedded ad forwarder pseudonyms are shown in Fig. 5. As discussed in Section IV-C, each ad packet, e.g., P_B, contains the pseudonyms of the upstream, current, and downstream ad forwarders, which are denoted as $P_B(A, B, C)$ in Fig. 5.

In the first place, the CC verifies the PF of $SRSU$, i.e., PF_{RSU}, by verifying the digital signatures of the ad packets embedded in PF_{RSU}. Once PF_{RSU} is verified as being valid, the CC can find the next downstream ad forwarder based on PF_{RSU} in the following sequence: The CC will first search for the PF of node A, i.e., PF_A, as shown in case 1 in Fig. 5. If PF_A is absent, the CC will search for PF_B, as shown in case 2. If PF_B is also absent, the CC will continue to search for the PF with the identifiers of both A and B in its first embedded ad packet, i.e., PF_C, as shown in case 3. If PF_C is also absent, the CC will search for the PF with the identifier of B in the first embedded ad packet, i.e., PF_D, as shown in case 4. Once the next PF, e.g., PF_A, is found, it will be verified regarding its embedded ad packets. Once PF_A is verified as being valid, it will be used as the basis to determine the next ad forwarder with similar procedures as previously mentioned. This way, starting from the SRSU, the CC can construct an ad forwarding chain with the honest ad forwarder in each hop.

Property Analysis: Assuming the trustworthiness of the SRSU, the downstream ad forwarders can be reliably and securely verified by the CC, even in the face of missing PFs or forged PFs. The ad forwarding chain can be constructed in cases of missing or invalid PFs in up to four consecutive hops. However, such cases may be very rare, due to the tendency of rational nodes to obtain their incentives. Moreover, by checking the time information in each PF, the CC can also detect duplicate ad forwarding in 2-D scenarios and only accept the valid PFs with the earliest timestamp for each hop.

One misbehaving node may launch a denial-of-service (DoS) attack by continuously sending invalid PFs with garbage content to the CC. However, if this node does not digitally sign its invalid PFs, they will be ignored by the CC. Otherwise, the CC may send the invalid PFs as a proof of its misbehavior to the VANET Authority, which can punish or even evict this misbehaving node with the help of reputation schemes [32], [34]. Thus, this DoS attack can be safely ignored in VAAD.

The communication overhead incurred by PF submission is bounded by the number of ad forwarders N_F for each ad rebroadcast, and each PF has a small size due to the absence of $DATA_{\mathrm{AD}}$. Similarly, the computation overhead of the CC is also bounded by N_F. In addition, similar to other infrastructure entities such as the Authority and SPs, the CC is a logical entity that can be physically implemented in a distributed way in VANETs to be scalable. Although interesting, the scalable implementation of these infrastructure entities is orthogonal to the research focus of this paper.

C. Query-Based Incentive Distribution

To enable each valid ad forwarder to obtain its incentive in a privacy-preserving way, a query-based incentive distribution algorithm is proposed here.

Specifically, the CC will create an E-cash [35], [36] voucher with a certain incentive for each ad forwarder. The E-cash voucher for each ad forwarder, e.g., node B, will be encrypted with the secret key SK_B, as established in PF_B. All encrypted E-cash vouchers for one ad will be published in a website

maintained by the CC. Each encrypted voucher will be labeled by the corresponding pseudonym (e.g., B), for each ad forwarder to identify its E-cash voucher based on its previous pseudonym.

This way, each E-cash voucher is only accessible to the intended ad forwarder. The query made by any ad forwarder with a new pseudonym will not reveal the connection between its pseudonyms, which is one critical requirement for privacy protection in VANETs. In addition, this query-based incentive distribution approach is much more efficient than any push-based approach, which inevitably involves flooding VANETs with E-cash vouchers since the location of any ad forwarder is unknown due to privacy protection.

VI. Discussions

A. Security Properties

Section V shows that VAAD supports secure and privacy-preserving incentive distribution to honest ad forwarders. In addition, VAAD can also ensure reliable and controllable ad dissemination in VANETs. Specifically, the secure packet format proposed in Section IV-C ensures authentic and undeniable ad disseminations in VANETs. Second, the incentive serves to facilitate honest ad forwarding of the rational nodes. The requested dissemination distance D_i can effectively control the cost, effect, and geographic range of ad dissemination.

The node misbehaviors can be easily detected and thwarted in VAAD. Specifically, in case that the current ad forwarder intentionally selects a very near downstream ad forwarder, such an unreasonable selection can be easily detected by its neighbors. In case the current forwarder pretends to be on the border of D_i and does not send out the ad packet, it can be easily detected by its one-hop neighbors based on the parameters in the ad packet. In 2-D scenarios, if one ad forwarder in the intersection mode only forwards the ad along one direction, it can be detected by the nodes on other road segments. In case that one ad forwarder forwards duplicate ads in the intersection mode, it can be detected by CC in verifying the PFs, as discussed in Section V-B.

From aforementioned discussions, a reputation scheme will be helpful to punish the detected malicious nodes in VAAD, which will be addressed in our future work.

B. Location Relevance Versus Content Relevance

As discussed in Section IV-A, DBG only concerns the location relevance of ads without considering their content relevance to the ad receivers. This design rationale can be justified by the broadcast nature of wireless communications and the dominating advertising methods in the real world. First, ad dissemination aims to notify both interested and potential customers of a particular service. Thus, it would limit the advertising effect to disseminate the ad to only interested vehicular nodes. Second, due to the broadcast nature of VANET communications, all nodes nearby one ad forwarder will overhear the ad packet regardless of its personal interests. Thus, it is reasonable to consider location relevance, instead of content relevance in VAAD.

C. Application Significance of VAAD

VAAD provides an incentive-centered architecture for SPs, VANET infrastructure, and vehicular nodes to trade off their conflicting requirements regarding ad dissemination. In particular, VAAD allows each SP to estimate and control the cost and effect of its ads, with which the SP can easily map its high-level advertising requirements to the system parameters in VAAD, as shown in Section VII-A. Thus, VAAD is a practical solution to VANET-based ad dissemination.

Essentially, VAAD provides an ad dissemination pattern that is similar to physical ad posters to exploit the location relevance of ads. In VAAD, the ads can be flexibly updated without involving costly human efforts. Thus, the virtual ad posters of VAAD are preferable to physical ad posters.

In addition, given that VANETs will be implemented in the future, VAAD does not require any additional hardware investment to vehicular nodes. In case the RSUs are too sparse at the initial stage of VANETs, lightweight ad hoc RSUs (adRSUs), as proposed in [4], can be temporarily deployed in specific regions to facilitate ad dissemination in VANETs.

VII. Performance Analysis and Simulations

In this section, the performance of VAAD will be analyzed and compared to that of SSD [20]. To examine the performance in various environmental scenarios, it is necessary to implement a large geographical deployment, which requires numerous vehicles and is generally too costly. Thus, instead of field test experiments, the theoretical analysis and simulations are usually applied to evaluate the protocol performance in VANETs, as in the existing work [37]–[40].

A. Controllability of Advertising Effect and Cost

With VAAD, the advertising cost and effect are controllable. In general, the theoretical number of ad forwarders N_{FT} indicates the cost of ad dissemination, whereas the theoretical number of ad receivers N_{RT} is a proper indicator of the effect of ad dissemination.

Given a gradient p and road segment length L, the expected (average) requested ad-dissemination length of each ad $E[D_i]$ can be estimated as follows in 1-D scenarios:

$$E[D_i] = \sum_{k=1}^{\infty} \Pr\{D_i = kL\} \times kL = L/(1-p). \quad (4)$$

Since the ad packet can be disseminated to two directions with respect to the SRSU, on average, the ad will cover $2E[D_i]$. Thus, given the average node density α (node/meter) and the average hop length d_a around the SRSU, the cost and effect of ad dissemination can be estimated as follows:

$$E[N_{FT}] = 2E[D_i]/d_a = 2L/\left[(1-p)d_a\right] \quad (5)$$

$$E[N_{RT}] = 2E[D_i] \times \alpha = 2L\alpha/(1-p). \quad (6)$$

TABLE II
COMMON SIMULATION PARAMETERS

Parameter	*Value*	*Parameter*	*Value*
R	300 m	Beacon Period	100ms
MAC	802.11a	Average velocity	30m/s
Bit-rate	6Mbps	Simulation Time	1000s

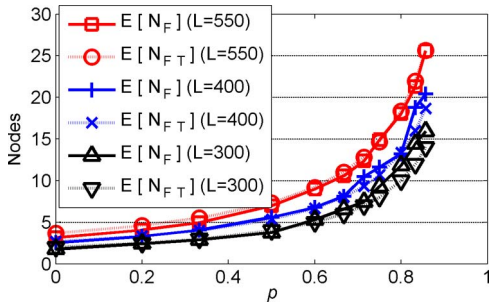


Fig. 6. Number of ad forwarders.

Based on (5) and (6), each SP can select proper p and L based on its specific cost budget and effect requirements.

In 2-D scenarios, D_i indicates the ad dissemination distance from the SRSU. Thus, the average area of the circular areas covered by this ad is

$$E\left[\pi D_i^2\right] = \sum_{k=1}^{\infty} \pi (kL)^2 (1-p) p^{k-1} = \pi L^2 (1+p)/(1-p)^2. \quad (7)$$

Thus, given the average road density β(meter/meter^2) around the SRSU, in 2-D scenarios, the cost and effect of ad dissemination in VAAD can also be estimated as

$$E[N_{FT}] = E\left[\pi D_i^2\right] \beta / d_a. \quad (8)$$

$$E[N_{RT}] = E[\pi D_i^2] \beta \alpha. \quad (9)$$

Thus, based on (7)–(9), each SP can estimate and control the cost and effect of its ad in 2-D scenarios.

To verify the aforementioned analysis, NS2-based simulations [41] are performed here with realistic vehicle mobility traces generated by MObility model generator for VEhicular networks [42]. Due to the similarity of IEEE 802.11a to DSRC [43] and its ready availability in NS2, we use IEEE 802.11a as the MAC protocol in our simulations. The simulation parameters are listed in Table II.

Highway (1-D) Scenario: In the highway scenario, 200 vehicles run in a road of length 10 km, with one RSU installed at one end of the road. Here, L is set to 300, 400, or 550 m, and p is set to 0.0, 0.2, 0.333, 0.5, 0.6, 0.667, 0.714, 0.75, 0.8, 0.833, or 0.857. Given each combination of (L, p), the theoretical number of ad forwarders $E[N_{FT}]$ and the actual number of ad forwarder $E[N_F]$ are shown in Fig. 6. To emphasize on the controllability of VAAD, network partitions are omitted here. The close match between $E[N_F]$ and $E[N_{FT}]$ in Fig. 6 indicates the effectiveness of VAAD in controlling the cost of ad dissemination.

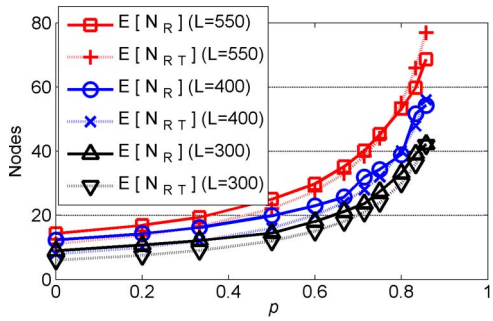


Fig. 7. Number of ad receivers.

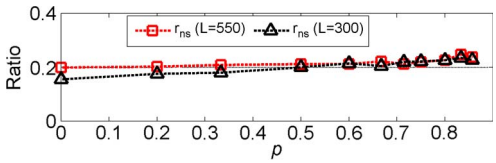


Fig. 8. Ratios of abnormal cases.

Similarly, in Fig. 7, the actual number of ad receivers $E[N_R]$ also closely matches the theoretical number of ad receivers $E[N_{RT}]$. Thus, VAAD effectively controls the effect of ad dissemination by properly configuring both p and L.

To reflect the impact of network partitions, in Fig. 8, the abnormal cases of network partitions are investigated. Here, r_{ns} is the percentage of ads running into a network partition. As shown in Fig. 8, r_{ns} is almost constant for each L, slightly increasing with the increase in p. Thus, while implementing VAAD, special care needs to be taken to decrease the impact of network partitions. For instance, the RSUs in VANETs may help forward the ads in the face of network partitions.

Downtown (2-D) Scenarios: Here, we present the simulation results of VAAD in a square area of 4000 m by 4000 m with five vertical roads and five horizontal roads. The SRSU is located at the center of this area. Node density α is 1 node per 100 m, and road density β is 0.0025 m per 1 m^2. The total number of vehicles is 400.

We set $L = 300$ m and change p from 0.1 to 0.8. Thus, the desired ad dissemination distance D_D changes from 330 to 1500 m, accordingly. The theoretical number of ad forwarders $E[N_{FT}]$, the actual number of ad forwarders $E[N_F]$, the theoretical number of ad receivers $E[N_{RT}]$, and the actual number of ad receivers $E[N_R]$ are shown in Fig. 9. When p is smaller than 0.6, the close matching of $E[N_F]$ to $E[N_{FT}]$ and $E[N_R]$ to $E[N_{RT}]$ shows that VAAD can control the cost and effect of ad dissemination in 2-D scenarios. The discrepancies between $E[N_F]$ and $E[N_{FT}]$, as well as between $E[N_R]$ and $E[N_{RT}]$, with $p > 0.6$, result from the limited size of our 2-D scenario. As p increases, the SRSU is more likely to set D_i larger than the radius of our simulation scenario, which is 2000 m. In such a case, the ad packet can only be forwarded to 2000 m away from the SRSU.

Overall, the aforementioned simulation results corroborate the effectiveness of VAAD in controlling the cost and effect of ad dissemination. By comparison, with its focus on secure incentive construction, SSD [20] does not support precise ad

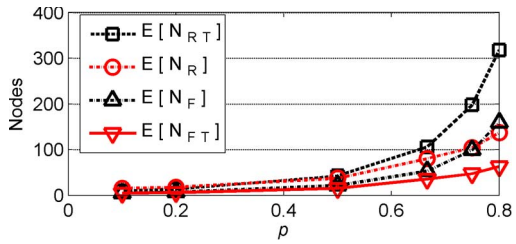


Fig. 9. Simulation results in 2-D scenario.

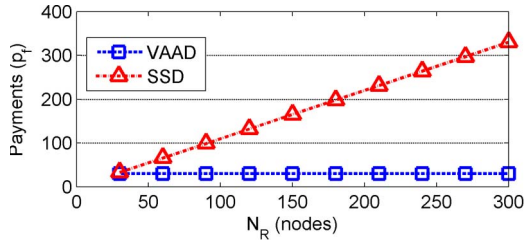


Fig. 10. C_V versus C_S.

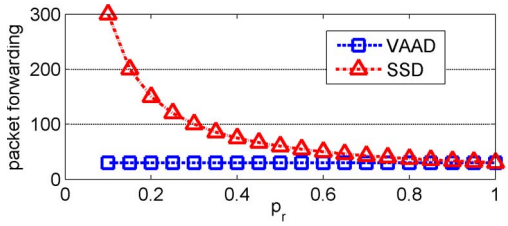


Fig. 11. O_V versus O_S.

cost and effect control. Specifically, in the level-free ad dissemination model of SSD, each node can freely forward the ad packets to its neighbors. In the n-level model, a node that has received the ad within n levels from SRSU can forward this ad. However, in both models, the numbers of ad forwarders and ad receivers cannot be estimated or controlled since each node can move around and send this ad to multiple receivers.

B. Cost and Overhead Comparisons

Here, we theoretically compare the cost and communication overhead incurred by SSD [20] and VAAD. For fair comparison, we assume that, in both SSD [20] and VAAD, the incentive given to each ad forwarder is p_f. In SSD, an incentive of p_r $(0 \leq p_r \leq p_f)$ will be given to each ad receiver, which generates a receipt for this ad.

Suppose that, in VAAD, an ad is forwarded by N_F ad forwarders and received by N_R ad receivers. Thus, the cost incurred by VAAD is

$$C_V = N_F \times p_f. \tag{10}$$

Similarly, suppose in SSD an ad is forwarded by N_F ad forwarders and results in N_R ad receipts. The cost of SSD is

$$C_S = N_R \times p_f + N_R \times p_r. \tag{11}$$

Equation (11) holds since, in SSD, the ad forwarder is rewarded based on the receipts it collects. Generally, each ad forwarder will result in multiple ad receivers, and therefore, $N_R \gg N_F$. Thus, C_S is much higher than C_V from (10) and (11).

For instance, let $N_F = 30$, and $N_R = 30, 60, \ldots, 270, 300$. Let $p_r = 0.1p_f$. As shown in Fig. 10, C_S is always larger than C_V since SSD will not only pay each ad forwarder but also pay each ad receiver generating a receipt. Thus, as the node density increases, N_R/N_T will also increase, and the discrepancy between C_S and C_V will become even larger.

In addition, the total communication overhead of VAAD O_V is only N_F ad forwarding. To estimate the communication overhead of SSD, we assume that each ad receiver will generate a receipt with a probability p_r/p_f. Thus, the ad forwarding in SSD is $O_S = N_F \times p_f/p_r$. Thus, O_S is higher than O_V as long as $p_r < p_f$. Furthermore, according to [20], each ad forwarding in SSD consists of one ad packet and one three-way handshake for each ad receipt. Overall, the overhead of SSD is much higher than that of VAAD to achieve the same advertising effect.

As an example, let $N_T = 30$ and $N_R = 150$. Let p_r change from 0.1 p_f to 1.0 p_f. As shown in Fig. 11, O_S is much higher than O_V, due to the fact that not every ad receiver will generate a receipt. As p_r increases, the probability of one ad receiver to generate a receipt increases, and O_S decreases to O_V. However, as previously discussed, bigger p_r results in larger cost in SSD. Thus, VAAD incurs smaller communication overhead than SSD in any scenarios.

Thus, SSD [20] results in higher incurred cost and communication overhead than VAAD. With a more realistic incentive model, VAAD is more cost effective and efficient in VANETs.

C. Impacts of L and p on VAAD

Given a desired ad dissemination distance (D_D), bigger p indicates more diversification of the ad rebroadcasts. In one extremity, $p = 0$ $(L = D_D)$ specifies that a constant distance $(D_i = L)$ is adopted for all ad rebroadcasts. As p increases, D_i is further diversified to allow the ad to be occasionally disseminated very far to give more preparation times to the coming vehicles. This diversification of D_i emphasizes on the location relevance of ads by forming an ad density gradient. Next, the impacts of L and p on the performance of VAAD will be analyzed and verified with simulations in 1-D scenarios, which provides useful guidelines for configuring p and L.

In the following simulations, the parameters in Table II are also adopted. With D_D fixed at 3000 m, L changes from 300 to 3000 m with a step size of 300 m.

Penetration Distance l_m: Here, l_m is defined as the maximal distance where the ad density is bigger than a threshold ε, as set by the SP. Thus, l_m indicates the effective ad dissemination distance over a long time period. According to the DBG algorithm, the jth road segment will have ad density p^j; therefore,

$$p^j \geq \varepsilon \Rightarrow j = \lfloor \log_p \varepsilon \rfloor \tag{12}$$

$$l_m = (j+1)L. \tag{13}$$

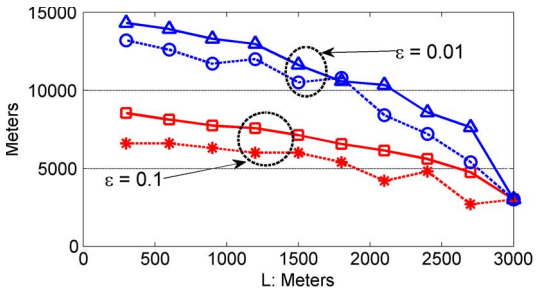


Fig. 12. l_m for both settings.

In (12) and (13), $p \in (0, 1)$. In Fig. 12, both the theoretical estimations and statistics obtained from simulations are shown for $\varepsilon = 0.01$ and $\varepsilon = 0.1$, respectively. Note that, in the simulations, when an ad reaches the end of the 10-km road, it will be broadcasted backward to simulate a longer road. The simulation statistics (solid lines) closely follow the theoretical estimations (dash lines), which justify our theoretical analysis. In addition, Fig. 12 shows that, as L increases, l_m will generally decrease due to smaller diversification of D_i.

Sensitivity to Network Partitions: Here, the sensitivity of $E[D_i]$ to network partitions regarding different L and p values is estimated. For simplicity, we assume that L_0 is the average distance before a network partition. We also assume that, when D_i is larger than L_0, the actual dissemination distance will be L_0; on the other hand, if D_i is not larger than L_0, the actual dissemination distance is D_i. Let $n = L_0/L$. Considering network partitions, the average ad dissemination distance $E[D_i^*]$ becomes

$$E[D_i^*] = \sum_{k=1}^{n} \Pr\{D_i = kL\}kL + \sum_{k=n+1}^{\infty} \Pr\{D_i = kL\}L_0$$

$$= \sum_{k=1}^{n} (1-p)p^{k-1}kL + \sum_{k=n+1}^{\infty} (1-p)p^{k-1}L_0$$

$$= D_D(1-p^n) = D_D(1-p^{L_0/L}). \tag{14}$$

From (14), as L increases to D_D (p decreases to 0), $E[D_i^*]$ will increase to approach D_D, indicating decreasing sensitivity to network partitions. This is consistent to our intuition that the less diversified D_i is, the less likely an ad rebroadcast will run into a network partition before it reaches D_i.

Probability of Missing All Ads (p_m): Let p_m denote the probability that one node passing by the SRSU will miss all ads. In reality, when the ad rebroadcast frequency f is smaller or bigger than v/D_D, where v is the average vehicle speed near the SRSU, the node movement has more significant impacts on p_m. Thus, to emphasize on the impacts of L and p, here, we consider the case where $f = v/D_D$.

For simplicity, assume that D_D is a multiple (m) of L, where m is a natural number. Thus, $p = 1 - 1/m$ from (4). First, we estimate $p_{m1}(c)$, the probability that a vehicle running away from the SRSU will receive no ad packet from the SRSU, with the initial condition that it is between cL and $(c+1)L$ away from the SRSU when the SRSU broadcasts the first ad packet. Thus, the probability that it misses the kth $(k = 1, 2, \ldots)$ ad packet from the SRSU can be estimated as

$$\Pr\{miss \quad kth \quad ad|c\} = \sum_{j=1}^{m(k-1)+c-1} (1-p)p^{j-1}$$

$$= 1 - p^{m(k-1)+c}. \tag{15}$$

From (15), we have

$$p_{m1}(c) = \prod_{k=1}^{\infty} \Pr(miss \quad kth \quad ad|c)$$

$$= \prod_{k=1}^{\infty} (1 - p^{(k-1)m+c}). \tag{16}$$

Numerical simulation shows that $p_{m1}(c)$ increases from 0 as c increases from 0 to $m-1$. In addition, $p_{m1}(m-1)$ increases and approaches a limit of 0.5 as m increases. For simplicity, assume that $p_{m1}(c)$ linearly increases as c increases. Then

$$p_{m1}(c) = 0.5 \times c/(m-1), \qquad c = 0, 1, \ldots, m-1. \tag{17}$$

By spatial symmetry, $p_{m1}(c)$ also indicates the probability that a node running to the SRSU will receive no ad, under the condition that it will be between cL and $(c+1)L$ away from the SRSU at the last ad packet. Assume that nodes are uniformly distributed along the timeline. Taking into considerations both sides of the SRSU

$$p_m = 1/m \sum_{c=0}^{m-1} [p_{m1}(c)p_{m1}(m-1-c)]. \tag{18}$$

As m increases, we can approximate $1/(m-1)$ with a continuous variable dx and $c/(m-1)$ with a continuous variable x. Then, (18) can be approximated with an integral as

$$p_m \doteq \int_0^1 0.5x \times 0.5(1-x)dx = 1/24. \tag{19}$$

Thus, from aforementioned analysis, p_m is bounded by 1/24 for any value of p. Thus, the impact of various p on p_m can be ignored.

VIII. Conclusion

With an incentive-centered architecture, VAAD allows different parties involved in ad dissemination to trade off their conflicting requirements. In particular, VAAD allows each SP to configure the geographic range, cost, and effect of its ad disseminations. In VAAD, the disseminated ad packets form a virtual ad poster around the SRSU to increase their location relevance. In addition, the secure and privacy-preserving cash-in algorithm encourages the rational vehicular node to participate in forwarding ad packets for the SPs.

Thus, VAAD supports secure ad dissemination in VANETs with pragmatic cost and effect control. Being more cost effective and efficient than existing advertising methods, e.g., ad dissemination based on cellular communications and roadside ad posters, VAAD shows appealing application potential in future VANETs.

In the future, we will design an effective and efficient reputation scheme to punish malicious nodes detected in VAAD. A lightweight E-cash scheme will also be adopted to efficiently and securely support financial transactions.

REFERENCES

[1] RITA, Washington, DC, Connectivity-The Evolving Paradigm for IntelliDrive, 2011.

[2] Z. Li, Z. Wang, and C. Chigan, "Security of vehicular ad hoc networks in intelligent transportation systems," in *Wireless Technologies in Intelligent Transportation Systems*, Y. Z. M.-T. Zhou and L. T. Yang, Eds. Hauppauge, NY: Nova Publ., 2011, pp. 133–174.

[3] M. Boban and O. K. Tonguz, "Multiplayer games over vehicular ad hoc networks: A new application," *Ad Hoc Netw.*, vol. 8, no. 5, pp. 531–543, Jul. 2010.

[4] Z. Li, C. Liu, and C. Chigan, "GPAS: A general-purpose automatic survey system based on vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 61–66, Aug. 2011.

[5] O. Riva, T. Nadeem, C. Borcea, and L. Iftode, "Context-aware migratory services in ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 6, no. 12, pp. 1313–1328, Dec. 2007.

[6] R. Handorean, R. Sen, G. Hackmann, and G.-C. Roman, "Context aware session management for services in ad hoc networks," in *Proc. IEEE Int. Conf. Services Comput.*, 2005, pp. 113–120.

[7] M. D. Dikaiakos, A. Florides, T. Nadeem, and L. Iftode, "Location-aware services over vehicular ad-hoc networks using car-to-car communication," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1590–1602, Oct. 2007.

[8] N. Klimin, W. Enkelmann, H. Karl, and A. Wolisz, "A hybrid approach for location-based service discovery in vehicular ad hoc networks," in *Proc. 1st Int. WIT*, Hamburg, German, 2004, pp. 1–5.

[9] C. Lochert, H. Hartenstein, J. Tian, H. Fussler, D. Hermann, and M. Mauve, "A routing strategy for vehicular ad hoc networks in city environments," in *Proc. IEEE Intell. Veh. Symp.*, 2003, pp. 156–161.

[10] C. Lochert, M. Mauve, H. Fubler, and H. Hartenstein, "Geographic routing in city scenarios," in *Proc. SIGMOBILE Mobile Comput. Commun. Rev.*, 2005, vol. 9, pp. 69–72.

[11] M. Nekovee and B. B. Bogason, "Reliable and efficient information dissemination in intermittently connected vehicular adhoc networks," in *Proc. IEEE 65th Veh. Technol. Conf.*, 2007, pp. 2486–2490.

[12] W. Wang, F. Xie, and M. Chatterjee, "Small-scale and large-scale routing in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 9, pp. 5200–5213, Nov. 2009.

[13] N. Cenerario, T. Delot, and S. Ilarri, "A content-based dissemination protocol for VANETs: Exploiting the encounter probability," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 771–782, Sep. 2011.

[14] C. Liu and C. Chigan, "RPB-MD: Providing robust message dissemination for vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 10, no. 3, pp. 497–511, May 2012.

[15] M. Torrent-Moreno, D. Jiang, and H. Hartenstein, "Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks," in *Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw.*, Philadelphia, PA, 2004, pp. 10–18.

[16] S. Eichler, C. Schroth, T. Kosch, and M. Strassberger, "Strategies for context-adaptive message dissemination in vehicular ad hoc networks," in *Proc. 3rd Annu. Int. Conf. Mobile Ubiquitous Syst.*, 2006, pp. 1–9.

[17] T. Kosch, C. J. Adler, S. Eichler, C. Schroth, and M. Strassberger, "The scalability problem of vehicular ad hoc networks and how to solve it," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 22–28, Oct. 2006.

[18] M. Sardari, F. Hendessi, and F. Fekri, "Infocast: A new paradigm for collaborative content distribution from roadside units to vehicular networks," in *Proc. 6th Annu. IEEE Commun. Soc. Conf. Sens., Mesh Ad Hoc Commun. Netw.*, 2009, pp. 1–9.

[19] A. Nandan, S. Tewari, S. Das, M. Gerla, and L. Kleinrock, "AdTorrent: Delivering location cognizant advertisements to car networks," in *Proc. IEEE/IFIP WONS*, 2006, pp. 1–10.

[20] S.-B. Lee, G. Pan, J.-S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," in *Proc. 8th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Montreal, QC, Canada, 2007, pp. 150–159.

[21] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security—Special Issue Security Ad-Hoc Sens. Netw.*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

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

[23] "Vehicle safety communications project: Task 3 final report: Identify intelligent vehicle safety applications enabled by DSRC," Nat. Highway Traffic Safety Admin., Washington, DC, U.S. Dept. Transp. DOT HS 809 859, Mar. 2005.

[24] B. K. Chaurasia, S. Verma, G. S. Tomar, and S. M. Bhaskar, "Pseudonym based mechanism for sustaining privacy in VANETs," in *Proc. 1st Int. Conf. Comput. Intell., Commun. Syst. Netw.*, 2009, pp. 420–425.

[25] J. Freudiger, M. Manshaei, J. Y. L. Boudec, and J. P. Hubaux, "On the age of pseudonyms in mobile ad hoc networks," in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[26] M. Gerlach and F. Guttler, "Privacy in VANETs using changing pseudonyms - Ideal and real," in *Proc. IEEE 65th Veh. Technol. Conf.*, 2007, pp. 2521–2525.

[27] E. Shi, A. Perrig, and L. Van Doorn, "BIND: A fine-grained attestation service for secure distributed systems," in *Proc. IEEE Symp. Security Privacy*, 2005, pp. 154–168.

[28] J. R. Douceur, "The sybil attack," in *Proc. 1st Int. Workshop Peer-to-Peer Syst.*, 2002, pp. 251–260.

[29] Z. Li, C. Liu, and C. Chigan, "VehicleView: A universal system for vehicle performance monitoring and analysis based on VANETs," *IEEE Wireless Commun. Mag.*, 2012, to be published.

[30] B. Blaszczyszyn, P. Muhlethaler, and Y. Toor, "Performance of MAC protocols in linear VANETs under different attenuation and fading conditions," in *Proc. 12th Int. IEEE Conf. Intell. Transp. Syst.*, 2009, pp. 1–6.

[31] G. Fairhurst and L. Wood, "Advice to link designers on link Automatic Repeat reQuest (ARQ)," Internet Eng. Task Force (IETF), Fremont, CA, IETF RFC 3366, 2002.

[32] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[33] S. Eichler, "Strategies for pseudonym changes in vehicular ad hoc networks depending on node mobility," in *Proc. IEEE Intell. Veh. Symp.*, 2007, pp. 541–546.

[34] Z. Li and C. Chigan, "Joint privacy and reputation assurance for VANETs," in *Proc. IEEE ICC*, Ottawa, ON, Canada, 2012, pp. 565–570.

[35] D. Chaum, "Blind signatures for untraceable payments," in *Proc. Int. Crytol. Conf.*, 1982, pp. 199–203.

[36] B. Lian, G. Chen, and J. Li, "A provably secure and practical fair E-cash scheme," in *Proc. IEEE ICITIS*, 2010, pp. 251–255.

[37] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A new VANET-based smart parking scheme for large parking lots," in *Proc. IEEE INFOCOM*, 2009, pp. 1413–1421.

[38] S.-T. Cheng, G.-J. Horng, and C.-L. Chou, "Using cellular automata to form car society in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1374–1384, Dec. 2011.

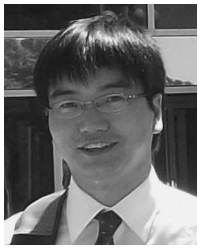
[39] F. Dion, J.-S. Oh, and R. Robinson, "Virtual testbed for assessing probe vehicle data in intellidrive systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 635–644, Sep. 2011.

[40] P. Fernandes and U. Nunes, "Platooning with IVC-enabled autonomous vehicles: Strategies to mitigate communication delays, improve safety and traffic flow," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 91–106, Mar. 2012.

[41] ISI, The Network Simulator - ns-2, Sep. 2, 2011. [Online]. Available: http://www.isi.edu/nsnam/ns/index.html

[42] K. Lan, Rapid Generation of Realistic Simulation for VANET, Feb. 13, 2007. [Online]. Available: http://lens1.csie.ncku.edu.tw/MOVE/index.htm

[43] B. S. Gukhool and S. Cherkaoui, "Handling handovers in vehicular communications using an IEEE 802.11p model in NS-2," *Int. J. Ultra Wideband Commun. Syst.*, vol. 1, no. 3, pp. 159–168, 2010.



Zhengming Li received the M.S. degree in control theory and engineering from Tsinghua University, Beijing, China, in 2005 and the Ph.D. degree in electrical engineering from Michigan Technological University, in 2012.

His research interests include security provisioning, privacy protection, and application design in vehicular ad hoc networks.

Congyi Liu received the M.S. degree in control theory and control engineering from Shanghai Jiao Tong University, Shanghai, China, in 2007. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Michigan Technological University, Houghton.

His research interests include data dissemination, data aggregation, and data collection in vehicular ad hoc networks.

Chunxiao Chigan received the M.S. and Ph.D. degrees in electrical engineering from the State University of New York, Stony Brook, in 2000 and 2002, respectively.

She is currently an Associate Professor with the Department of Electrical and Computer Engineering, Michigan Technological University, Houghton. Her research interests include cyber security and information assurance, vehicular ad hoc networks, cognitive radio networks and security, wireless ad hoc and sensor networks, and vehicle-to-grid communications. Her research has been funded by the Department of Defense, industry, and the National Science Foundation (NSF).

Prof. Chigan serves as an Associate Editor for the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS. She received the NSF CAREER Award in 2007.