Peer-to-Peer Netw. Appl. (2014) 7:737–742
DOI 10.1007/s12083-012-0178-y

Securing one-way hash chain based incentive mechanism for vehicular ad hoc networks

Joon-Sang Park · Seung Jun Beak

Received: 18 July 2012 / Accepted: 29 October 2012 / Published online: 8 November 2012

Abstract One of the most promising applications of yet to come vehicular ad hoc networks (VANETs) is commercial advertising. However, in order to realize commercial advertising over VANET, proper incentives and security mechanisms must be taken into consideration due to the existence of selfish and/or malicious users in the real-world scenario. In this paper, we propose a secure incentive scheme for VANET advertising systems based on one-way hash chains. We also analyze the advertisement propagation behavior in our VANET advertising system using a mathematical model.

Keywords Vehicular ad hoc networks · Incentives · Security · Public Key Infrastructure

1 Introduction

Vehicular ad hoc networks (VANETs) are wireless networks for smart vehicles on the road. In such networks, vehicles equipped with short-range radios, e.g., DSRC [1], communicates with other nearby vehicles or with roadside infrastructure. The technology is mainly driven by safety enhancement needs but it is envisioned to play an important role as "communication networks on the road" and provide numerous interesting services in the near future [2–4]. Among them, one of the most promising applications is to disseminate commercial advertisements via car-to-car communication, e.g., Electronic Coupon Systems [5] and FleaNet [6]. In such systems, vehicles disseminate advertisements by forwarding them to other vehicles while moving. This vehicular dissemination system is very effective for advertisement, since a vehicle itself moves from place to place so that it can forward the advertisement whenever new vehicles move into its vicinity. One of the problems of such systems is that they just simply assume nodes' cooperativeness: each vehicle naively forwards the advertisements repeatedly for a certain time period if they are asked to. However, in reality, there may be selfish nodes not wanting to disseminate advertisements for free. Even for naive nodes, there is no clear reason why they should help disseminate those advertisements for the benefit of others. Thus to deploy such vehicular advertisement system in real-world scenarios, proper incentives mechanisms should be taken into consideration.

To realize such a vehicular commercial advertising system, a secure incentive framework leveraging a Public Key Infrastructure (PKI) called Signature-Seeking Drive (SSD) has been proposed in [7]. Inspired by a micro-payment scheme [8] and a charging/rewarding scheme [9], SSD charges for the provision of advertising service and rewards participating users as an incentive using the notion of *virtual cash*. In SSD, once a moving vehicle obtains a legitimate advertisement from an advertiser, it starts to disseminate the advertisement to other users come across while moving. When disseminating the advertisement, the vehicle collects from the advertisement receiving vehicles *receipts* which later can be redeemed at *virtual cashier* for *virtual cash* as a reward for its service. Also the predefined amount of the cash is also reserved for each receipt-providing user. Later, an advertiser defrays the cost for the virtual cash induced by the advertisement, which stimulates cooperation among users.

J.-S. Park (✉)
Department of Computer Engineering,
Hongik University,
72-1 Sangsoo-Dong, Mapo-gu,
Seoul 121-791, Korea
e-mail: jsp@hongik.ac.kr

S. J. Beak
College of Information and Communications,
Korea University,
Anam-dong 5-ga, Seongbuk-gu,
Seoul 136-713, Korea

Among a series of incentive mechanisms proposed as parts of SSD, the incentive mechanism based on one-way hash functions has security problems. In order for the system to work as designed, users must voluntarily follow instructions given by the system, i.e., lack of coercive measures against illegitimate indirect (secondhand) deliveries of advertisements. Thus, malicious users can manipulate the system to incur unexpected high charges to advertisers. In fact, its security was intentionally compromised for simplicity. To address the problem, we propose in this paper a "secure" incentive scheme based on one-way hash chains which can effectively prohibit unauthorized propagation of advertisements and thus a advertiser can manage the total cost for publishing an advertisement. Similar to SSD, our scheme does not rely on tamper-proof hardware (e.g., [10, 11]) or game theoretic approaches (e.g., [5, 12–15]), yet leverages a PKI to provide a secure incentive mechanism for cooperative nodes.

The rest of this paper is organized as follows. We describe our secure incentive system in Section 2, an analytic evaluation of proposed scheme is given in Section 3, and we draw conclusions in Section 4.

2 Securing incentive schemes for advertising in VANET

In this section we first describe our target VANET environment and assumptions and then present our secure incentive scheme for advertising in VANET.

In VANET advertising systems, with the help of inter-vehicle communications, advertisers' goal is to disseminate their advertisements within certain time period and/or within a certain vicinity. Advertisers probably want to use VANET advertising system to propagate their advertisements, targeting a large number of potential customers. However, from the perspective of normal users in VANET, those commercial advertisements are only for the benefit of the advertisers and they are exploiting users' resources for their own profit. Users probably want some type of incentive to stimulate active participation. Thus, a graceful compromise between these two sides is to charge advertisers and to pay users as an incentive for active cooperation. Advertisers pay charges for the usage of network resources which are provided by normal users in VANET.

Utilizing PKI, we assume that each registered vehicle keeps its own certificate, in other words, public/private key pair issued by a Certificate Authority (CA). In addition to protect users' privacy, each vehicle may obtain temporary IDs, i.e., anonymous public/private key pairs. We assume that any nodes cannot obtain a certificate for another entity from CA. Every commercial advertisement requires obtaining permission from an authority called Vehicular Authority (VA). VA authorizes every advertisement and maintains the records of all the vehicular advertisement payment transactions. Each vehicle is preloaded with the VA's public key as well as the CA's public key.

There are two types of uncooperative users, selfish users and malicious users. Selfish nodes try to maximize their own benefits, whereas malicious nodes have the intention of disrupting some part or even the whole network. A complete incentive system should deal with both selfish nodes and malicious ones. Our scheme pursues secure incentives to stimulate cooperation among users and at the same time preventing attackers from disrupting the system.

We use the following notations throughout this paper: u,v are principals; C_u is u's certificate by CA; K_u^+ is u's public key; K_u^- is u's private key; $M1|M2$ is the concatenation of messages $M1$ and $M2$; $H(M)$ is hash of M, e.g., SHA-1 [16]; $\{M\}_{K_u^-}$ is u's digital signature on (hashed) M; AD_s is an advertisement by company S. We also use $u \rightarrow v{:}M$ to denote that u sends message M to v, and $u \rightarrow *{:}M$ to denote that u broadcasts M.

In summary, once vehicle u agrees to disseminate an advertiser I's advertisement, u continues to forward it to any newly-encountered vehicle v for a certain time period. Advertisement-receiving vehicle v, in return, may provide a digitally-signed receipt for u. These receipts are exchangeable with virtual cash at the virtual cashier (e.g. gas station). Also, a predefined amount of the cash is reserved for v. The virtual cashier sends all the transaction records to VA. Then, VA charges I such virtual cash induced by the advertisement, and I pays for what stimulates cooperation among users, as an incentive for both advertising node u and receipt-providing node v.

Approval for advertisement Every commercial advertisement to be published over the VANET advertisement platform must be approved by VA. An advertiser I, e.g., an restaurant, gets its advertisement AD_I certified by a VA as follows:

$$\begin{aligned} I \rightarrow VA: &\quad C_I, AD_I, n, \alpha, \{AD_I|n|\alpha\}_{K_I^-}. \\ VA \rightarrow I: &\quad \{AD_I|I|H^n(\alpha)\}_{K_{VA}^-}. \end{aligned}$$

where C_I is I's certificate, n is the propagation level limit, α is a random number generated by I, and $H^n(\alpha)$ is a value applied an one-way hash function H n times on α. By the propagation level limit, we mean how many other users can be involved before an advertisement is delivered to a final user. If it is set to 1, then the only vehicles that have received an advertisement directly from the advertiser are allowed forward the advertisement to others. If the value if greater than 2, indirect deliveries of ads or so called multi-level dissemination is permitted. Figure 1 shows an example of multi-level dissemination. It allows vehicle v to reuse the ad from u, so v can make its virtual cash by forwarding this ad to other vehicle x. Then, x can also reuse and advertise it to others. The propagation level limit is a factor to the cost and dissemination speed. In general, the higher the value is the faster the dissemination speed will be. With I's digital signature on AD_I, VA authenticates I's identity. After reviewing I's request, VA issues I an *ad-permit* $\{AD_I|I|H^n(\alpha)\}_{K^-_{VA}}$. This notion of ad-permit prevents malicious users from abusing the system with dummy/unauthorized advertisements. We assume that each vehicle is preloaded with the VA's public key as well as the CA's public key.

Agreement with advertiser I contacts with each approaching vehicle u as follows:

$$\begin{aligned}
I \rightarrow * :\quad & C_I, AD_I, n, \alpha, \{AD_I|I|H^n(\alpha)\}_{K^-_{VA}}.\\
u \rightarrow I :\quad & C_u, \{AD_I\}_{K^-_u}.\\
I \rightarrow u :\quad & \left\{\{AD_I|I|H^n(\alpha)\}_{K^-_{VA}}|u|n-1|H(\alpha)\right\}_{K^-_I}.
\end{aligned}$$

where C_I is I's certificate, n is the propagation level limit, α is a random number, and $H^n(\alpha)$ is a value applied an one-way hash function H n times on α.

When u receives AD_I, it first checks whether AD_I has been properly approved by VA. This process involves applying H n times on α. If the advertisement is legitimate, u may respond to this advertisement by sending back its certificate. Then, after verifying u's identity, I provides u with a *voucher* $\left\{\{AD_I|I|H^n(\alpha)\}_{K^-_{VA}}|u|n-1|H(\alpha)\right\}_{K^-_I}$ for u's exclusive use. Without this voucher, u cannot redeem collected receipts at the virtual cashier. Other vehicles fail to share this voucher, since it is tied with u's identity.

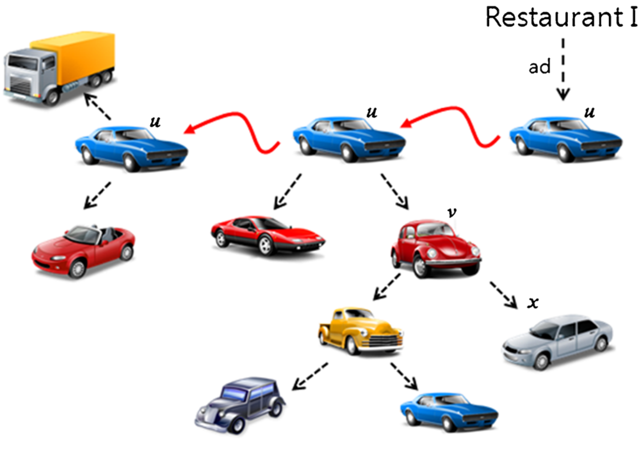

Fig. 1 Propagation of ad

Advertisement dissemination Hoping to make as much virtual cash as possible, u disseminates AD_I to any neighboring vehicle v after reducing n by 1 and applying H on α as follows:

$$\begin{aligned}
u \rightarrow * :\ & C_u, AD_I, I, n-1, H(\alpha)\\
& ,\left\{\{AD_I|I|H^n(\alpha)\}_{K^-_{VA}}\right\}_{K^-_u}.\\
v \rightarrow u :\ & C_v, \{AD_I|u|n-1|H(\alpha)\}_{K^-_v}.\\
u \rightarrow v :\ & C_I,\\
& ,\left\{\{AD_I|I|H^n(\alpha)\}_{K^-_{VA}}|v|n-2|H^2(\alpha)\right\}_{K^-_u}\\
& ,\left\{\{AD_I|I|H^n(\alpha)\}_{K^-_{VA}}|u|n-1|H(\alpha)\right\}_{K^-_I}.
\end{aligned}$$

Where C_u and C_v are u's and v's certificates, respectively. v checks both u's identity and AD_I's legitimacy by applying H $n-1$ times on $H(\alpha)$. If everything is correct, v may respond to this advertisement, with an incentive in mind, by providing its certificate and a digitally-singed receipt for u in which the level index "$n-1$'" is locked. Only the receipts with the valid level index (allowed for the advertising node) are accepted by VC for redemption. Then, u hands over the voucher received from I and a new voucher generated specifically for v by locking its id in the voucher which are both needed for v when receipt redemption. v verifies these vouchers by applying H one time on hashed α in the latter voucher to see if it is the same as the value in the former voucher. This is to enforce the level index advanced only by one at each step/hop and thus the propagation level limit set by the advertiser. u may continue forward the ad in the hope of collecting as many receipts as possible.

In fact, u hands over v the vouchers only when $n-1$ is greater than zero, i.e., v is allowed to disseminate AD_I. Otherwise, the transaction is complete after v issues u a receipt. If $n-1$ is greater than zero, then v may forward AD_I to any approaching vehicle x after reducing the level index $n-1$ by 1 and applying H on $H(\alpha)$ as follows:

$$\begin{aligned}
v \rightarrow * :\ & C_v, AD_I, I, n-2, H^2(\alpha)\\
& ,\left\{\{AD_I|I|H^n(\alpha)\}_{K^-_{VA}}\right\}_{K^-_v}.\\
x \rightarrow v :\ & C_x, \{AD_I|v|n-2|H^2(\alpha)\}_{K^-_x}.\\
v \rightarrow x :\ & C_u\\
& ,\{\{AD_I|I|H^n(\alpha)\}_{K^-_I}|x|n-3|H^3(\alpha)\}_{K^-_v}\\
& \left\{\{AD_I|I|H^n(\alpha)\}_{K^-_{VA}}|v|n-2|H^2(\alpha)\right\}_{K^-_u}
\end{aligned}$$

where C_v and C_x are v's and x's certificates, respectively. The verification process undergone by x is the same as the one performed by u when it has communicated with u. If $n-2$ is still non-zero, x can reuse AD_I. In this way, AD_I can be propagated until it reaches level n.

Now let z be a vehicle located at k^{th} level in the propagation tree. That is, the ad has been handed over k times before it researches z. Then, z forwards the ad to any neighboring vehicle as follows (given $k<n$):

$$\begin{aligned}
z \rightarrow * &: C_z, AD_I, I, n-k, H^k(\alpha) \\
&, \left\{ \{AD_I|I|H^n(\alpha)\}_{K_{VA}^-} \right\}_{K_z^-}. \\
a \rightarrow z &: C_a, \left\{AD_I|z|n-k|H^k(\alpha)\right\}_{K_x^-}. \\
z \rightarrow a &: C_y \\
&, \left\{ \{AD_I|I|H^n(\alpha)\}_{K_I^-}|a|n-k-1|H^{k+1}(\alpha) \right\}_{K_z^-} \\
&, \left\{ \{AD_I|I|H^n(\alpha)\}_{K_{VA}^-}|z|n-k|H^k(\alpha) \right\}_{K_y^-}
\end{aligned}$$

where y is the vehicle form which z has received the ad and C_y, C_z and C_α are y's, z's and a's certificates, respectively. Again, if $n-(k+1)$ is still non-zero, a can reuse AD_I and forward it to any vehicles.

Receipt redemption Each vehicle should redeem its collected receipts before the specified time of AD_I to get rewarded for its service. Every certified ad has its own term of validity specified in it. Before the expiration of AD_I, u may return its collected receipts to any nearby virtual cashier VC as follows:

$$\begin{aligned}
u \rightarrow VC :\ & C_u, C_I, AD_I, I \\
&, \{\{\{AD_I|I|H^n(\alpha)\}_{K_{VA}^-}|u|n-1|H(\alpha)\}_{K_I^-}\}_{K_u^-}, R_u. \\
& R_u = (C_v, \{AD_I|u|n-1|H(\alpha)\}_{K_v^-}), \ldots \\
v \rightarrow VC :\ & C_v, C_u, C_I, AD_I, I \\
&, \left\{ \left\{ \{AD_I|I|H^n(\alpha)\}_{K_{VA}^-}|v|n-2|H^2(\alpha) \right\}_{K_u^-} \right\}_{K_v^-} \\
&, \left\{ \{AD_I|I|H^n(\alpha)\}_{K_{VA}^-}|u|n-1|H(\alpha) \right\}_{K_I^-}, R_v. \\
& R_v = \left(C_x, \{AD_I|v|n-2|H^2(\alpha)\}_{K_x^-} \right), \ldots \\
x \rightarrow VC :\ & C_x, C_v, C_u, AD_I, I \\
&, \left\{ \left\{ \{AD_I|I|H^n(\alpha)\}_{K_{VA}^-}|x|n-3|H^3(\alpha) \right\}_{K_v^-} \right\}_{K_x^-} \\
&, \left\{ \{AD_I|I|H^n(\alpha)\}_{K_{VA}^-}|v|n-2|H^2(\alpha) \right\}_{K_u^-}, R_x. \\
& R_x = \left(C_y, \{AD_I|x|n-3|H^3(\alpha)\}_{K_y^-} \right), \ldots
\end{aligned}$$

where R_u, R_v, and R_x are the receipts collected by u, v, and x, respectively. Note that, to redeem receipts, each vehicle, x for example, is requested to hand in two vouchers, one is the voucher issued for x and the other is the voucher issued to its predecessor, i.e., the vehicle who issued a voucher to x. On reception of redemption request, VC first checks (1) the due date of AD_I, (2) vehicles' identity, and (3) the legitimacy of the vouchers. Those are verified with each vehicle's digital signature on its voucher and by applying H $n-k$ times on hashed $H^k(\alpha)$ where k=1, 2, 3, … Also VC verifies that the hashed α is the former voucher is the value same as the hashed α in the latter voucher after applying H one more time. Then VC examines whether the vehicle, u for instance, has never redeemed u's voucher for AD_I at any other virtual cashier before, by inquiring of VA about u's previous record. Each VC is connected with a VA that maintains the records of all the vehicular ad payment transactions. Then VC verifies the legitimacy of each receipt received from each distinct node in R_u. VC sends all of this data to a VA that keeps vehicular ad records. Now u earns as much virtual cash as the number of the valid receipts in R_u. The predefined amount of the cash may be given to each receipt-providing vehicle in R_u to simulate active participation of every involving party in this scheme. Later VA charges restaurant I such virtual cash induced by AD_I. Since VA keeps all the records of vehicular ad payment transactions, u can redeem its voucher for AD_I only once.

3 Performance evaluations

In this section, we investigate advertisement propagation behaviors in the network, i.e, how fast ad propagates throughout the network. To this end, we first develop a mathematical model based on Ordinary Differential Equations (ODE).

Let us assume that there are N nodes moving in a restricted $L\times L$ region according to a random mobility model such as Random WayPoint (RWP) model. In such a setting, the pairwise inter-node meeting rate λ can be estimated by the following formula [17]:

$$\lambda = \frac{8wdv}{\pi L^2}$$

where w=1.3685 is a constant specific to the mobility model which is in our case RWP, d is the radio transmission range, and v is the node speed (assuming that every node is moving at the same speed.)

Then, let $n(t)$ be the number of nodes at time t possessing the ad and we have

$$\frac{dn(t)}{dt} = \lambda U(N - n(t)) \tag{1}$$

where

$$U = \begin{cases} n(0) & \textit{if one} - \textit{level advertisement}, \\ n(t) & \textit{if unrestricted advertisement}. \end{cases}$$

with initial condition $n(0)=K$ which is the number of nodes that possess an ad from the start. In case of one-level advertisement, the propagation level limit is set to one and in case of unrestricted advertisement, there is no the propagation level limit. In words, at time t, the total number of ad-possessing nodes $n(t)$ is increased by $\lambda U(N-n(t))$ since a new node that does not have the ad encounters any ad-possessing node with the rate of λU and there are ($N-n(t)$) new nodes and U ad-possessing nodes in the area. To model multi-level advertising but not unrestricted, we define $n_l(t)$ to be the number of level-l nodes at time t possessing the ad and we have

$$\frac{dn_l(t)}{dt} = \lambda n_{l-1}(t)(N - n(t))$$

with

$$n(t) = \sum_{l=0}^{M} n_l(t).$$

where M is the highest level allowed. The total number of ad-possesing node is the sum of nodes at all levels.

Figure 2 plots $n(t)$, the total number of ad-received nodes, as a function of time. We assume that there are 1000 nodes moving at the speed of $30km/s$ in the terrain sized $20\times 20km^2$ and the radio transmission range is $250m$. Among 1000 nodes, 10 nodes carry the ad from the start. As we can see in the figure, as the propagation level limit increases, an ad tends to propagate more rapidly in the network. When the limit is 5, the ad covers the entire network in about 10 min. When the limit is 3, the ad propagation completes in 20 min. In the mean time, if the propagation level limit is set to one, the ad is propagated over the network very slowly and the ad is delivered to only 70 % of the total nodes even after 120 min have past. Although not reported in the figure, we can see easily from the model that as λ increases, the ad propagation speed increases. That is, one can enhance the ad propagation speed by increasing the vehicle speed and the radio transmission range, i.e., λ.

4 Discussion and related work

In VANETs, to implement the primary "road safety" applications, a centrally-managed infrastructure (possibly including a PKI) becomes an essential part. Also a PKI turns out to be a suitable way for satisfying security requirements in car-to-car communication [18, 19] since power unlimited computing resource equipped in each vehicle is capable of processing digital signatures [20] and asymmetric authentication mechanisms do not require a preliminary handshake which is usually not acceptable in inter-vehicle communication. Our incentive scheme utilizes a PKI and the assistance of the centralized administration, e.g., CA, to achieve its security goal: users are being paid the right amount they deserve and advertiser are properly charged for their uses of the system. Similar to SSD, our schemes effectively prevent the colluding nodes from sharing/fabricating their vouchers or collected receipts, since each of those is cryptographically tied to the only one holder's identity. Also, malicious nodes fail to launch DoS attacks, e.g. generating dummy ad, since receiving nodes discard such unauthorized ads without a VA's signature on it. The integrity of ad content is protected so that they cannot modify the ad, e.g. free-riding attack [9]. We assume that malicious nodes have the same capability as normal users. However, once malicious users cheat a VA into issuing ad-permits with fake identities, they are able to disrupt the system without being charged for what they invoke. Thus, the management of a VA as well as CA is the critical issue in our scheme.

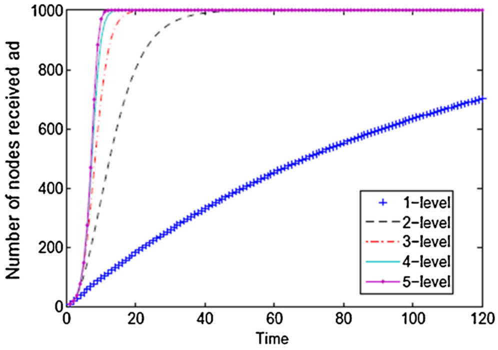

Fig. 2 Advertisement propagation behavior

In our scheme, a user has to collect nodes' certificates as well as their signed receipts when disseminating ads, which raises privacy concerns. Thus, to protect privacy against unauthorized observers, each user can utilize its temporary IDs, whose certificates have short lifetimes, e.g., a few minutes with the reanonymizer [18], so that each user changes its signing key periodically. This helps prevent third parties from tracking the real identities of communicating vehicles.

Several incentive schemes stimulating cooperation among selfish nodes have been proposed for mobile ad-hoc networks. One possible approach is to use tamper-proof hardware [10, 11] to manage and protect virtual credit system. In such systems, to motivate each individual node to participate in the network each relaying node is being paid some virtual credit. Other approaches utilize reputation-based schemes, e.g., [21], in which each node monitors and keeps track of the reputation of neighboring nodes to detect and isolate from the network uncooperative nodes. Also, several researches have taken game theocratic approaches to investigate non- cooperative scenarios [5, 12–15]. By manipulating the communication parameters in the network, e.g. the amount of gain per forwarding, those schemes are designed to stimulate cooperation among selfish nodes. However, these incentive schemes have potential to backfire since it may offer an incentive to cheat the system in order for users to gain further benefits if poorly implemented in practice as pointed out in [22].

5 Conclusions

In this paper we have presented a secure incentive scheme based on one-way hash function for commercial advertising in VANETs. Our system leverages a PKI to provide a secure incentive mechanism that can stimulate cooperation among nodes and countermeasures against malicious nodes. Also we have analyzed the performance of our proposed scheme using a mathematical model.

Acknowledgments This work was supported in part by the National Research Foundation of Korea Grant funded by the Korean Government (2010-0005334, 2010-0027410).

References

1. 5.9 GHz Dedicated Short Range Communications (DSRC). http://grouper.ieee.org/groups/scc32/dsrc/index.html.
2. Luo J, Hubaux JP (2005) A survey of research in inter-vehicle communications. Securing Current and Future Automotive IT Applications, pp 111–122, Springer-Verlag.
3. Xu Q, Mark T, Ko J, Sengupta R (2004) Vehicle-to-vehicle safety messaging in DSRC. In Proc. ACM VANET.
4. Yang X, Liu J, Zhao F, Vaidya N (2004) A vehicle-to-vehicle communication protocol for cooperative collision warning. In Proc. MobiQuitous.
5. Kangasharju J, Heinemann A (2006) Incentives for electronic coupon systems. In Proc. ACM Workshop MobiShare.
6. Lee U, Lee J, Park J-S, Gerla M (2010) FleaNet: a virtual market place on vehicular networks. IEEE Trans Veh Technol, 59(2).
7. Lee S-B, Park J-S, Gerla M, Lu S (2012) Secure incentives for commercial ad dissemination in vehicular networks. IEEE Trans Veh Technol, 61(6).
8. Jakobsson M, Hubaux JP, Buttyan L (2003) A micro-payment scheme encouraging collaboration in multi-hop cellular networks. In Proc. Financial Crypto.
9. Ben Salem N, Buttyan L, Hubaux J-P, Jakobsson M (2003) A charging and rewarding scheme for packet forwarding. In Proc. ACM MobiHoc.
10. Buttyan L, Hubaux JP (2002) Stimulating cooperation in self-organizing mobile ad hoc networks. ACM J Mob Netw (MONET).
11. Vogt H, Gartner FC, Pagnia H (2003) Supporting fair exchange in mobile environments. ACM Mob Netw J (MONET).
12. Chen T, Zhu L, Wu F, Zhong S (2011) Stimulating cooperation in vehicular ad hoc networks: a coalitional game theoretic approach. IEEE Trans Veh Technol 60(2)
13. Felegyhazi M, Hubaux J-P, Buttyan L (2006) Nash equilibria of packet forwarding strategies in wireless ad hoc networks. IEEE Trans Mob Comput
14. Wei H-Y, Gitlin RD (2005) Incentive mechanism design for selfish hybrid wireless relay networks. ACM Mob Netw J.
15. Zhong S, Chen J Yang YR (2003) Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks. In Proc. IEEE INFOCOM.
16. Eastlake D, Jones P (2001) US Secure Hash Algorithm 1 (SHA1). RFC 3174.
17. Groenevelt R, Nain P, Koole G (2005) The message delay in mobile ad hoc networks. In Proc. Performance.
18. Parno B, Perrig A (2005) Challenges in securing vehicular networks. In Proc. HotNets-IV.
19. Raya M, Hubaux J-P (2005) The security of vehicular ad hoc networks. In Proc. ACM SASN.
20. Zarki ME, Mehrotra S, Tsudik G, Venkatasubramanian N (2002) Security issues in a future vehicular network. In Proc. EuroWireless.
21. Liu Y, Yang YR (2003) Reputation propagation and agreement in mobile ad-hoc networks. In Proc. IEEE WCNC.
22. Huang E.Crowcroft J, Wassell I (2004) Rethinking incentives for mobile ad hoc networks. In Proc. ACM SIGCOMM Workshop on Practice and Theory of Incentives in Networked Systems.

Joon-Sang Park received the M.S. degree in computer science from the University of Southern California in 2001 and the Ph.D. degree in computer science from University of California, Los Angeles (UCLA) in 2006. He was a postdoctoral researcher at UCLA and is currently an Assistant Professor with the Computer Engineering Department, Hongik University, Seoul, Korea. His research interests include routing and MAC protocols in mobile ad hoc and sensor networks, and network coding.

Seung Jun Baek received B.S. degree in electrical engineering from Seoul National University in 1998. He earned M.S. and Ph.D. degree in electrical and computer engineering from University of Texas at Austin in 2002 and 2006. Since 2009, he has been an assistant professor at Dept. of Computer and Communications in Korea University. His research interests include cellular networks, heterogeneous networks, cognitive radio and sensor networks.