A Hybrid Trust Management Framework for Vehicular Social Networks

Rasheed Hussain[1(✉)], Waqas Nawaz[1], JooYoung Lee[1], Junggab Son[2], and Jung Taek Seo[3]

[1] Institute of Informatics, Innopolis University, Innopolis, Russia
{r.hussain,w.nawaz,j.lee}@innopolis.ru
[2] Department of Mathematics and Physics, North Carolina Central University, Durham, USA
json@nccu.edu
[3] College of Information Security, Soonchunhyang University, Asan, South Korea
seojt@sch.ac.kr

Abstract. This paper addresses the trust management problem in the emerging Vehicular Social Network (VSN). VSN is an evolutionary integration of Vehicular Ad hoc NETwork (VANET) and Online Social Networks (OSN). The application domain of VSN inherits the features of its parental VANET and OSN, providing value-added services and applications to its consumers, i.e. passengers and drivers. However, the immature infrastructure of VSN is vulnerable to security and privacy threats while information sharing, and hard to realize in the mass of vehicles. Therefore, in this paper, we particularly advocate for communication trust establishment and management during information exchange in VSN. First, we establish functional architectural frameworks for VSN that are based on the underlying applications. Second, based on these frameworks, we propose two trust establishment and management solutions, i.e. email-based social trust and social networks-based trust, to target different sets of applications. Third, we discuss the contemporary research challenges in VSN. Our proposed scheme is a stepping stone towards the secure and trustworthy realization of this technology.

Keywords: VANET · Social networks · Vehicular Social Network (VSN) · Trust · Reputation · Security · Privacy

1 Introduction

Vehicular Ad hoc NETwork (VANET) is poised to offer the drivers and passengers with a safe, at least fail safe, reliable, and infotainment-rich driving environment. From the research results in the field of vehicular networks (semi-autonomous) and driverless (autonomous) cars, it can be easily speculated that intelligent transportation system (ITS) technologies, which are realized through VANET, will be soon pervading our highways. There are few challenging issues

H.T. Nguyen and V. Snasel (Eds.): CSoNet 2016, LNCS 9795, pp. 214–225, 2016.
DOI: 10.1007/978-3-319-42345-6_19

that are keeping the stakeholders and investors at bay from deploying these technologies on a mass scale. These issues include security, privacy, trust, framework design, initial deployment, data and user privacy, to name a few [17].

The mobility patterns, based on space and time, are predictable in VANET and linked to online social networks (OSNs). For example, the traffic tends to be dense during rush hours because people are going to office in the morning and coming back home in the evening, which is not the case for non-peak hours. This phenomena develops a unique social relationships among neighbors who tend to share same interests and/or likely schedule. The recent developments in OSNs gives rise to the concept of VSN [19] by providing a preferred mean of sharing social activities among VANET users. Consequently, many VSN applications are developed for this purpose such as Tweeting car[1], SocialDrive [9], Social-based navigation (NaviTweet) [14], CliqueTrip [5], and GeoVanet. Beside the technological advancements, it is essential to look at the social perspective of VANET [3,4].

The credibility of both the stakeholders and the information shared through OSN in VANET infrastructure using VSN applications is a challenging task. The former is achieved through tools and methods from cryptography and public-key infrastructure (PKI), and the later cannot be guaranteed with the first line of defense, i.e. traditional PKI-based approach. The credibility of information can be indirectly measured through trust evaluation and management. Recently, a number of studies were conducted to look into the possibility of merging VANET with social networks and harvest the features of both technologies to enrich the application space of ITS [19]. A plethora of techniques proposed various solutions for trust establishment in VANET [1,2,6,10,11,13,15,16,18,20]. However, there is a significant gap between stakeholder and information trust. Specifically, the data level trust is overlooked by existing studies. To overcome these issues, we proposed architectural frameworks for VSN. Further, we establish two trust methods, namely email-based and social network-based trust, to guarantee the credibility of information in VSN.

The structure of the rest of this paper is organized as follows: Sect. 3 describes functional architectural frameworks for VSN. Our proposed trust management scheme is outlined in Sect. 4. We discuss the unique VSN research challenges in Sect. 5 followed by concluding remarks and future directions in Sect. 6.

2 Related Work

Trust is one of the many challenges in VANET. A number of studies have proposed various solutions for trust establishment in VANET. Node/entity trust is achieved in VANET through well-established cryptographic solutions. The cryptographic mechanisms help to prove the legitimacy of the source of communication. In other words, secure and efficient authentication mechanisms guarantee node trust in VANET [6,16,18,20]. Furthermore, trust management schemes

[1] http://www.engin.umich.edu/college/about/news/stories/2010/may/caravan-track-hits-the-road.

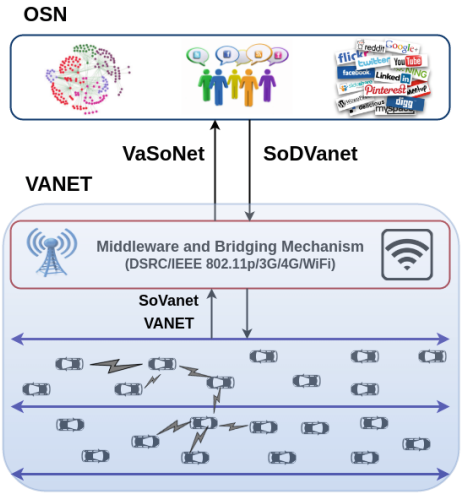

Fig. 1. VSN network and communication model

have also been implemented to build trust among the VANET users for information exchange [1,2]. In [15], the authors consider both data trust and node trust, and propose an attack-resistant trust management solution for vehicular networks. They achieve data trust through data collection from multiple sources (vehicles) and node trust through functional approach and recommendation approach. Moreover, a trust quantification mechanism is also proposed in [13]. Another email-based social trust establishment scheme has been proposed by Huang et al. [11]. Our email-based trust management in VSN is inspired by [11]. Huang et al. proposed a situation-aware trust framework in [10]. It includes an attribute-based policy control model for highly sporadic VANET, which is a proactive trust model to build trust among VANET nodes, and an email-based social network trust system to enhance trust among users. It is worth noting that the research community has focused on node/entity trust in VANET where the sender is judged based on the confidence of trust. A very small attention has been given to the data trust. In this paper we try to minimize the gap between node trust and data trust.

3 Functional and Architectural Frameworks of VSN

This section comprehensively discusses the network and communication model, taxonomy of VSN application areas, followed by potential architectural frameworks for VSN.

3.1 Network and Communication Model

The network and communication model for our proposed scheme is shown in Fig. 1. Social networks have their own setup and they run both desktops

and mobile versions. On the other hand, VANET is based on the dedicated short-range communication (DSRC) which mandates V2V and V2I communication. Vehicular nodes and roadside units are equipped with on-board units (OBUs) and tamper-resistant hardware (TRH). TRH is responsible for storing the security-related keys and other cryptographic material. OBUs send out different kinds of messages that include frequent beacon messages, service requests, key update requests, warning messages, and so forth. In order to bridge vehicular networks with the OSN, we have a number of options and roadside units (RSUs) is one of them. Today's high-end 3/4G network capable cars can also send and/or receive data to/from OSN to VANET. For instance, mobile devices with social network applications can connect to vehicle through WiFi and Bluetooth protocols.

3.2 Taxonomy

There are many application domains that benefit from VSN either directly or indirectly. Some of these application domains include entertainment, information exchange, diagnostic/control, health-care, platooning, cooperative cruise control, crowdsourcing, cooperative navigation, content delivery, social behavior, clustering-based communication, and vehicular clouds [19]. The communication among vehicles is the first entry point to the social networking paradigm, because both follow the same baseline principle of real world communication. Therefore, the information exchange is rendered as social interaction among vehicles. In order to understand the aforementioned application domains, we outline a detailed taxonomy of these applications based on varying architectures of VSN. We divide VSN into three functional architectural frameworks namely Social Data-driven vehicular networks (SoDVanet), Social VANET (SoVanet), and Vanet data-driven Social Networks (VaSoNet). Figure 2 outlines the taxonomy of VSN applications based on the underlying framework. These frameworks encompass the potential application domains from vehicular communications to user behavioral perspective.

3.3 Social Data-Driven Vehicular Networks (SoDVanet)

In SoDVanet framework, the existing vanet infrastructure uses social data obtained from users. Therefore, this framework broadens the application space and offers more services to pure vanet users. The SoDVanet architecture assumes that both vanet and social networks are established and there is a bridging mechanism to integrate these two in a seamless fashion. To be precise, vanet uses data from the available social network for its specific class of applications and provides the required services to the users. The integration is user-centric because every vanet user rely on its social network direct (friends) or multi-hop contacts (friends of friends) depending upon the required degree of connectivity. For instance, a comprehensive social data-driven information system would help the vanet users to be updated for certain events on the road, city, and/or across the

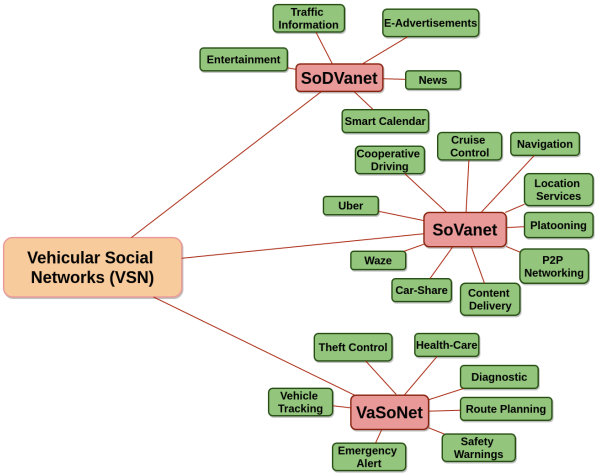

Fig. 2. Taxonomy of VSN applications

country. We can achieve this through a pull-based strategy at vanet infrastructure where the information shared by users in social networks is collected by the car and present it to the user based on his/her preferences.

3.4 Social VANET (SoVanet)

Vehicular nodes communicate with each other through different types of messages, for instance beacons and warning messages. Beacons are shared with neighbors and with infrastructure for cooperative awareness. The nature of these messages determine the social behavior among vehicles at communication and application level. Eventually, this results in realization of a number of applications through vehicular social communications. Besides beacons, vehicle also share critical information such as warning message as a result of some designated incident on the road, black ice on the pavement, ambulance approaching warning, traffic jam warning. Additionally, vehicle users can also share their experience related to daily social activities, e.g. experiences about a restaurant, availability of parking lots, new movies in the theatre. We call SoVanet as infrastructureless social network, because vehicles use existing vanet infrastructure and use social parameters for information exchange.

3.5 Vanet Data-Driven Social Networks (VaSoNet)

OSN users leverage the data obtained from vehicular communications in VaSoNet framework. The data obtained from VANET infrastructure is related to transportation. There are different variations for this communication paradigm; however, the most interesting one is the inquiry of transportation related information ubiquitously through VANET infrastructure. A certain query is executed

either in a centralized (at the server), or distributed fashion (by the nodes in the area of interest). For instance, before leaving home on a busy national holiday, one would like to know the current traffic situations on the road. The communication model of this framework is based on an efficient and secure bridging mechanism between OSN and VANET. A well defined mechanism is required at first place to authenticate the data sources in VANET and to preserve both user and location privacy. This paradigm comes with a unique challenge to stimulate the VANET nodes to share their experience and/or data, e.g. pictures-on-demand, real time traffic information, in correspondence with OSN queries.

4 Proposed Hybrid Trust Management Scheme

In this section we outline our proposed hybrid email-based and social network-based trust management scheme for the aforementioned VSN frameworks.

4.1 Baseline Overview

The health of information shared among nodes in VSN, is of paramount importance and cannot be achieved through traditional cryptographic techniques. Therefore we employ a trust management mechanism to make sure that the exchanged information is healthy and trustworthy. In the light of the fact that most of the users use email as a mean of communication, therefore we use the frequency of email interactions for trust calculation. In order to calculate peer trust, users look into the email interactions with neighbors. If the node is in the trusted list of the receiver node, then the information is likely to be trusted, otherwise there are a number of other options, for instance generating a query about the trust value of the sender node and/or looking into the social relations of the sender, and so forth. We particularly focus on the 2-hop trust propagation where the trust query propagates to friends and friends of friends. The nodes also maintain their peer trust based on personal interactions with the neighbors and if needed, share this trust information with neighbors. The users also calculate trust based on their social interactions through OSN and depending on application, they calculate the resultant trust from intermediate trust values.

4.2 System Initialization

In order to enable email-based trust, department of motor vehicles (DMV) initializes the OBU by performing a number of operations. First the user enters its anonymized email address and DMV registers it against the user. DMV also issues a number of pseudonyms $\{Ps_1^u, Ps_2^u, Ps_3^u, \ldots Ps_l^u\}$ to the user u. Furthermore, DMV issues public private key pair to each pseudonym $<PK_{Ps_i}^u, SK_{Ps_i}^u>$ and another master secret key SK_u which is derived from the email ID, E_u. The email ID E_u of user u serves as public key which it shares with the neighbors. DMV shares the trapdoor of the pseudonyms with revocation authorities (RAs) as well which will be used in revocation process. Due to space limitation, we

refer the readers to [12]. Each user also runs a local email agent that connects to email service provider. The user maintains its contacts in different groups such as family (fm), friends (fr), acquaintances (aq), and work (wr). In email-based trust, certain groups such as family, is static changes to family group are less likely while others will be dynamic. An absolute confidence value c_i is assigned to each group where i is the group. In the dynamic groups, the nodes can earn the privilege to upgrade to a different group with higher c_i. It is also to be noted that, $c_{fm} > c_{fr} > c_{wr} > c_{aq}$ which defines the preferences. There is also a baseline unknown confidence c_U which is assigned to the contacts who are either first timers or unknown.

4.3 Hybrid Trust Management in VSN

Our proposed trust management is composed of two modules, email-based trust calculation and social network-based trust calculation module. Based on application, these modules will work in adaptive and robust manner. For instance email-based trust can be ideal for the applications in SoDVanet and social network-based trust can be used for applications in VaSoNet. Trust mechanism is divided into three processes, trust bootstrap, trust calculation and evaluation, and trust query. We describe these processes in detail.

Trust Bootstrap. Bootstrapping of trust information is the first step before the real communication among users. Every user maintains three lists namely Known friends list (KFL), anonymous friends list (AFL), and random encounter list (REL). KFL contains the information about the friends that are known either through social networks or emails. The real distinction among friends is done through the aforementioned confidence value c_x where x is degree of closeness. AFL contains information about acquaintances developed through either vehicular communications, social networks, or emails. Lastly the lowest level of relation is the random encounter through vehicular communications or emails. The definition of random encounter is debatable; however, for the sake of understanding we argue that communications carried out with neighbors for less than a defined threshold t_σ, will be placed in REL, where σ is the lowest threshold for which the nodes must be communicating with each other to get the level of AFL. At the system initialization every node populates KFL and AFL (based on immediate previous experience) and an empty REL. These lists store the information against anonymous pseudonyms instead of real identities, whereas in case of KFL, a certain degree of node information is also known. Pseudonyms become handy in case of AFL where the receiving node is not sure about the real identity and the trust level is in its infancy. Moreover the pseudonyms serve other purposes like preserving conditional privacy and revocation when needed.

Trust Calculation and Evaluation. There are two kinds of trust evaluations, local trust evaluation through received messages and the recommendation from neighbors as a result of mutual communication. The trust calculation mechanism

can be either sender-centric or receiver-centric. Local trust is receiver-centric whereas the recommendation can be both sender-centric or receiver-centric. In case of sender-centric, the receivers of the message calculate the trust value for the sender and in case of receiver-centric, the receiving node calculates trust value for the source of the message. For our proposed scheme, we consider sender-centric trust where a node waits for confidence values that it accumulates for itself from the neighbors.

Each node i calculates the trust value for its neighbor j based on two factors: (i) encounters (number of beacons η_b to be more precise) that i had with j. (ii) endorsement for j by its neighbors as a result of event message generated/broadcast by j. The net trust is calculated as follows:

$$\tau_j^i = \alpha \times \eta_b + (1 - \alpha) \times \sum_{i=1}^{n} \tau_e \times T_j^e$$

τ_j^i is the trust value calculated for node j by node i. α is the priority factor (weight) for the means of trust calculation (value between 0 and 1). In this case, we argue that the direct encounters carry more weight for the trust calculation than the endorsement of the neighbors. τ_e is the endorser's own trust value perceived from neighbors and T_j^e is the trust value endorsed by endorser e for the node j. It is worth noting that these values are obtained through group query-response process. The direct communication with the nodes will give more confidence to node i to calculate local trust value for the neighbors. Therefore the condition $\alpha > (1-\alpha)$ must hold. For the nodes in KFL, the trust calculator signs their certificates and pseudonyms with highest confidence. Whereas for the AFL nodes, the trust calculator signs the certificates with confidence $c_{AFL} < c_{KFL}$. The value of c_{AFL} will vary depending on the current neighborhood status of the node. For the nodes in REL, the certificates will be signed with a value of baseline confidence c_{REL}. The relation $c_{KFL} > c_{AFL} > c_{REL}$ must hold during the trust calculation.

In the email-based trust evaluation, every node assigns the trust to the nodes based on which list they currently belong to. For nodes in KFL, the trust calculator node assigns the fully-trusted status. In other words, if $n_i \in \{KFL\}$ and the contact frequency is above a threshold (certain emails in a specified amount of time) then $\tau_i = FullyTrusted$. On the other hand, for AFL, the trust calculator assigns the trust value based on heuristics from the previous trust value that was possessed by the node in question. There is a base trust value for AFL denoted by τ_{base}. If $n_i \in \{AFL\}$ then $\tau_i = \tau_{prev} + \tau_{cur}$, and $\tau_{prev} = \tau_{base} + \tau_{cur}$. This calculation is recursive and the only limit is the upper-bound of the AFL and REL. It is worth noting that the value of $\tau_{previous}$ will be between the base value for AFL and the base value for KFL. In other words, the maximum trust value of the nodes in AFL cannot exceed the base value of KFL. Similarly the social network-based trust calculation is same except for the lists management where only family and best friends are fully trusted while the trust of other nodes will depend on the frequency of communications. It is to be noted that if the credentials of a node are legitimate then the trust calculator will sign the

credential; however, the trust value will be calculated according to the aforementioned mechanism. Need for efficient interaction among social network, vehicular network and email service is essential for the trust management solution. The provision of intermediary service among these networks is out of scope of this paper.

Transitive Global Trust (Trust Query). In order to get a geographically-controlled global view of the neighbor's trust, a cooperative approach is employed where a node generates trust query to its immediate neighbors (including RSU). The query contains the email ID of the query originator, its pseudonym, and other credentials that will prove the legitimacy of the node. This query is broadcasted over DSRC channel. When the neighbors receive such query, first of all, they check for the validity of the cryptographic material in the query that includes certificate verification and validation. This is done by applying public key of the DMV/trusted party to the certificate. Then the receiver also checks for the validity of the pseudonym and certificate which can be checked through pseudonym revocation list (PRL) and/or certificate revocation list (CRL). We assume that an efficient PRL and CRL mechanisms are already in place [7,8]. After credential verification, the node traverses through its lists to determine the trust value for the node in the query. If the node is found, its trust value is sent back to the query originator along with the confidence value and signature of the responder. The query originator accumulates all the replies and updates the trust status of the node in the query. More precisely the query originator combines the trust values from the neighbors and calculates the net trust value for the node in the query. However if the node is not in the list of the responder, and the responder also received message from the node in query, then the responder seconds the query and show the interest to know the trust value of the node in query as well.

5 Research Challenges in VSN and Open Questions

5.1 Deployment

VANET is on the verge of deployment whereas OSN is fully deployed with unbelievably huge number of users and still growing. There are a number of problems that have caused the impeded momentum in VANET deployment. Few prominent issues include security, privacy, hardware, and lack of infrastructure. The deployment of VSN will face additional problems that are unique. For instance, investors will be reluctant to put their huge investment at stake. Therefore, at the first deployment stage, the traditional off-the-shelf hardware will become handy. More insight is needed to counter these issues at the very beginning of VSN deployment.

5.2 Security of Information Exchange

The security of information exchange is important in traditional VANET and OSN; however, in case of VSN the information exchange may violate user privacy.

On the other hand, the level of user privacy may be different in different applications. Therefore, the context information must be taken into account before preserving user and location privacy in VSN. It is also worth noting that the revocation mechanisms will vary from application to application in VSN.

5.3 Cross-Platform Conditional Privacy

The level of privacy is hard to generalize and seems application dependent in VSN. Moreover, the semantics of user privacy are different in OSN and VANET. Therefore, the cross-platform applications must take the privacy requirements into account while using data and preserve the user and/or location privacy accordingly. This phenomenon is going to be a daunting challenge in VSN and will require a thorough investigation.

5.4 Audit and Incentives

Most of the VSN applications are cooperative in nature where the data is collected through cooperation among nodes. However, selfish behavior from legitimate nodes is still not out of question. Therefore, a secure, efficient, and privacy-aware incentives mechanism is essential to stimulate active participation of the nodes.

5.5 Information Update/Decay

With the passage of time, the size of lists and their trust values will grow exponentially. Deep insight is required to decide on the frequency of the updates, to the lists, and the trust values. In order to find optimum frequency, the traffic scenario, spatial and temporal statistics must be taken into account. Moreover, the calculated trust values are not permanent and subject to change depending on the behavior of the neighbors. Therefore, the lifetime parameter of trust value is of paramount importance to guarantee the scalability of trust management scheme. The trust value should be valid for a certain amount of time after which the nodes will need to re-establish the trust. Determining the optimal time during is also an open problem.

5.6 Mobility vs Social Factors

In VANET, the mobility of vehicles is restricted to the road networks that will likely exhibit in VSN as well. Whereas in traditional OSN, there is no such restriction (although the behavior of users is still predictable). The data shared between VANET and OSN will definitely help the application to grow and provide the consumers with better services, but may also impact the social values of the users in both networks. For instance, profilation, user behavior, and social interests are prone to be abused as a result of such integration. Therefore, clear distinction is necessary between sensitive users' data and application data.

6 Conclusions and Future Work

In this paper, we aimed at a new paradigm shift referred to as vehicular social network (VSN) and proposed application-based architectural frameworks. First we proposed the application taxonomy of VSN and then three architectural frameworks namely Social Data-driven vehicular networks (SoDVanet), Social VANET (SoVanet), and Vanet data-driven Social Networks (VaSoNet). Furthermore, we proposed trust management system for VSN which leverages two approaches, email-based and social network-based trust management. In email-based trust management, the nodes calculate the trust values for neighbors based on the frequency of their email communication. The nodes also leverage social distinction among neighbors in terms of family, friends, work, and acquaintances. We also proposed social network-based trust management scheme for VSN. When nodes calculate the trust values for the neighbors, they consider the possibility of social relation with those neighbors through online social networks. Based on the nature of relation, respective trust value is calculated for the neighbor. In the proposed system, a node can also query trust status from its neighbors. We also outlined the research issues and open questions in VSN. We aim to implement the reputation system based on the real-world data and work on the optimization of scheme selection to incorporate trust scalability in VSN.

References

1. Abumansoor, O., Boukerche, A.: Towards a secure trust model for vehicular ad hoc networks services. In: Global Telecommunications Conference (GLOBECOM2011), pp. 1–5. IEEE, December 2011
2. Alriyami, Q., Adnane, A., Smith, A.K.: Evaluation criterias for trust management in vehicular ad-hoc networks (VANETs). In: 2014 International Conference on Connected Vehicles and Expo (ICCVE), pp. 118–123, November 2014
3. Cunha, F.D., Vianna, A.C., Mini, R.A.F., Loureiro, A.A.F.: How effective is to look at a vehicular network under a social perception? In: 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 154–159, October 2013
4. Cunha, F.D., Maia, G.G., Viana, A.C., Mini, R.A., Villas, L.A., Loureiro, A.A.: Socially inspired data dissemination for vehicular ad hoc networks. In: Proceedings of the 17th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, MSWiM 2014, NY, USA, pp. 81–85 (2014). http://doi.acm.org/10.1145/2641798.2641834
5. Ekler, P., Balogh, T., Ujj, T., Charaf, H., Lengyel, L.: Social driving in connected car environment. Proc. Eur. Wirel. Conf. **2015**, 1–6 (2015)
6. Feiri, M., Pielage, R., Petit, J., Zannone, N., Kargl, F.: Pre-distribution of certificates for pseudonymous broadcast authentication in VANET. In: 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), pp. 1–5, May 2015
7. Ganan, C., Munoz, J.L., Esparza, O., Mata-Diaz, J., Alins, J., Silva-Cardenas, C., Bartra-Gardini, G.: RAR: risk aware revocation mechanism for vehicular networks. In: 2012 IEEE 75th Vehicular Technology Conference (VTC Spring), pp. 1–5, May 2012

8. Haas, J.J., Hu, Y.C., Laberteaux, K.P.: Efficient certificate revocation list organization and distribution. IEEE J. Sel. Areas Commun. **29**(3), 595–604 (2011)
9. Hu, X., Leung, V.C., Li, K.G., Kong, E., Zhang, H., Surendrakumar, N.S., TalebiFard, P.: Social drive: a crowdsourcing-based vehicular social networking system for green transportation. In: Proceedings of the Third ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, DIVANet 2013, NY, USA, pp. 85–92 (2013). http://doi.acm.org/10.1145/2512921.2512924
10. Huang, D., Hong, X., Gerla, M.: Situation-aware trust architecture for vehicular networks. IEEE Commun. Mag. **48**(11), 128–135 (2010)
11. Huang, D., Zhou, Z., Hong, X., Gerla, M.: Establishing email-based social network trust for vehicular networks. In: 2010 7th IEEE Consumer Communications and Networking Conference, pp. 1–5, January 2010
12. Hussain, R., Kim, D., Tokuta, A.O., Melikyan, H.M., Oh, H.: Covert communication based privacy preservation in mobile vehicular networks. In: Military Communications Conference, MILCOM 2015, pp. 55–60. IEEE, October 2015
13. Kim, Y., Kim, I., Shim, C.Y.: Towards a trust management for vanets. In: The International Conference on Information Networking (ICOIN 2014), pp. 583–587, February 2014
14. Lequerica, I., Longaron, M.G., Ruiz, P.M.: Drive and share: efficient provisioning of social networks in vehicular scenarios. IEEE Commun. Mag. **48**(11), 90–97 (2010)
15. Li, W., Song, H.: Art: an attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. **17**(4), 960–969 (2016)
16. Lo, N.W., Tsai, J.L.: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. IEEE Trans. Intell. Transp. Syst. **PP**(99), 1–10 (2016)
17. Qu, F., Wu, Z., Wang, F.Y., Cho, W.: A security and privacy review of VANETs. IEEE Trans. Intell. Transp. Syst. **16**(6), 2985–2996 (2015)
18. Shao, J., Lin, X., Lu, R., Zuo, C.: A threshold anonymous authentication protocol for VANETs. IEEE Trans. Veh. Technol. **65**(3), 1711–1720 (2016)
19. Vegni, A.M., Loscr, V.: A survey on vehicular social networks. IEEE Commun. Surv. Tutorials **17**(4), 2397–2419 (2015)
20. Wang, F., Xu, Y., Zhang, H., Zhang, Y., Zhu, L.: 2FLIP: a two-factor lightweight privacy-preserving authentication scheme for VANET. IEEE Trans. Veh. Technol. **65**(2), 896–911 (2016)