Towards Trustworthy Vehicular Social Network

Authors: Qing Yang and Honggang Wang

http://dx.doi.org/10.1109/MCOM.2015.7105668

Q. Yang and H. Wang. "Towards Trustworthy Vehicular Social Networks", IEEE Communication Magazine, June, 2015, Volume: 53, Issue: 8 pp. 42-47.

http://x.doi.org/10.1109/MCOM.2015.7180506

Towards Trustworthy Vehicular Social Networks

Qing Yang, *Member, IEEE,* and Honggang Wang, *Senior Member, IEEE*

***Abstract*—Wireless vehicular networks offer the promise of connectivity to vehicles that could provide a myriad of safety- and driving-enhancing services to drivers and passengers. With wireless technology available on each car, it is expected that huge amounts of information will be exchanged between vehicles or between vehicles and roadside infrastructure. Due to defective sensors, software viruses, or even malicious intent, legitimate vehicles might inject untrustworthy information into the network. Besides relying on the public key infrastructure (PKI), this article proposes a social network approach to study trustworthy information sharing in a vehicular network. We first cover recent research progress in measuring direct trust and modeling indirect trust in online social networks then discuss how to apply them to vehicular social networks despite several pressing research challenges.**

***Index Terms*—Vehicular social network, direct trust, indirect trust, trustworthy information sharing.**

I. Introduction

Emerging wireless technologies enable vehicles to connect to each other to form a vehicular network through wireless channels and share traffic- or entertainment-related information to provide improved safety and pleasure to drivers and passengers. Besides existing wireless technologies (e.g., Bluetooth), various connectivity solutions such as dedicated short range communication (DSRC), cellular network, and WiFi are being bundled with OEM manufactured cars. Potential applications of networking vehicles include enhanced driving safety, smart roadside information systems, and environment-friendly transportation. In fact, the global connected car market shipments are expected to reach 59.86 million units and are likely to reach $98.42 billion by 2018 [1]. The existing and expected consumers demands and mandates are the major drivers for the connected vehicle market.

Various information are exchanged between cars in a vehicular network, including traffic jam, road constructions, incidents/crashes, road conditions and weather alerts, so it's important for a vehicle/driver to distinguish trustworthy from untrustworthy data. Vehicles sharing factual information with others are considered to be trustful, while those sending false information are distrustful. Currently, most research on trustworthy information sharing in vehicular networks rely on the public key infrastructure (PKI). Although PKI builds the first line of defense, it is possible for legitimate vehicles to send untrustworthy information due to defective sensors, computer viruses, and even for malicious reasons. Untrustworthy information sent by distrustful vehicles have the potential to become the most harmful data within a vehicular network, e.g., a driver might report wrong parking information to ensure he can park in the desired parking lot. A vehicular network, on the other hand, is also a mobile social network where vehicles meet each other to establish friendship-like relations and thus are embedded in a social structure. Therefore, an interesting question arises: *Is it possible to achieve a trustworthy vehicular network by applying the research findings about trust in social networks to vehicular networks?*

II. Vehicular Social Network

The terminology vehicular social network (VSN) was coined in [2]. A VSN connects vehicles which are physically close to each other and enables them to take advantage of their proximity to form a tightly-coupled, ad-hoc, and virtual world. This definition only considers the social connections between vehicles that are in each other's communication range. However, a VSN could be defined in a broader sense as the network of physically or virtually connected vehicles which are interested in sharing information for a common purpose or benefit. In such a network, physical and virtual connections between vehicles can be built via DSRC (dedicated short range communication), cellular networks, and Cloud [3].

Recently, the development of VSNs has gained momentum, which is coming largely from various applications of VSNs in people's daily lives. Fig. 1 categorizes existing VSN applications based on the physical and social distances between drivers. A driver can interact with others with different levels of familiarity, varying from family members to acquaintances (or even strangers). These people could be within the driver's car, nearby the car, or far away. With the help of a VSN, the driver can efficiently share information with others including, but not limited to, (1) having fun with *CarPlay* in a car (with the family), 2) sharing a restaurant review with friends via *FourSquare*, (3) tracking locations of family members by *Life360*, (4) scheduling a carpool with co-workers by *KarPooler*, (5) sharing his location in real time with acquaintances through *Glympse*, (6) sharing a ride and splitting the cost with another person who requests a ride along a similar route by *UberPool*, (7) cooperatively driving with nearby cars, and (8) sharing traffic-related information to strangers via *Waze*. Some of the above-mentioned systems, e.g., FourSquare, can actually provide services to drivers with various social and physical distances.

While the authors believe VSN will become popular within families and between close friends, it will mature when drivers are able to share information with strangers because more drivers are participating in VSNs. Therefore, this article focuses on the technical challenges of realizing trustworthy information sharing between stranger vehicles in VSNs.

A. Social Connections Between Vehicles

To understand how and why stranger vehicles are socially connected in a VSN, we first revisit the lifecycle of relationships among humans in traditional social networks. The

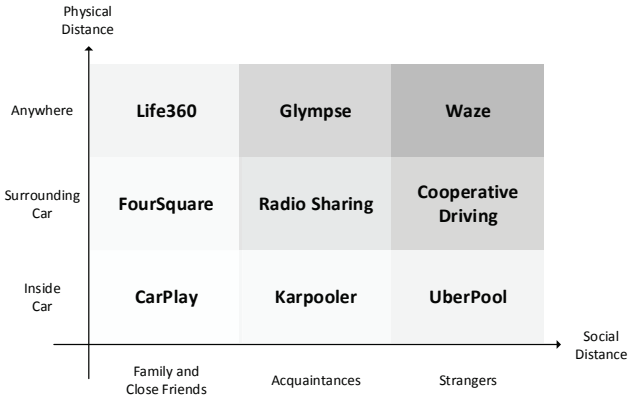

Fig. 1. Applications of VSN categorized by physical and social distances

lifespan of such a relationship can be broken into three stages: (1) a weak connection is created, (2) a weak connection is cultivated and becomes a strong one, and (3) a strong connection is maintained and a weak connection is terminated. At each stage, a connection could be created, cultivated, and maintained only when two people both have the desire to further their relationship.

In a VSN, it is evident that drivers desire to share information with each other, which has been demonstrated in the Waze.com, one of the world's largest community-based traffic and navigation system. However, it is unclear whether this desire leads to a social network among vehicles. Therefore, it is necessary to investigate the lifecycle of relations in traditional social networks and compare them to the counterparts in a VSN.

At the first stage, weak connections in traditional social networks are created from communities or existing social networks. If two persons share a common community (e.g., a dancing club), the likelihood that they create a connection becomes significantly large. Another way of building new connections is through a person's existing social network, e.g., your friend might introduce you to one of his friends. In VSNs, a car could connect with another if (1) they encounter (within the communication range) others on the road, and (2) have the common interest about shared information. While vehicles exchanging messages, their local social connections could also be shared, so it is highly possible for a vehicle to create virtual connections to its "friends' friends."

At the second stage, a weak connection becomes a strong connection when people in tradition social networks have the chance to interact with each other and cultivate their relationship. In VSNs, two vehicles frequently encountering and sharing information with each other (e.g., parking in the same parking lot) have the chance to build a weak connection into a strong one.

At the third stage, strong connections in traditional social network are maintained while weak connections are terminated. In the context of VSNs, strong connections are maintained if and only if two vehicles keep sharing mutually-beneficial information.

B. Construction of Vehicular Social Networks

A VSN can be constructed in centralized or distributed ways. In the centralized solution, a social connection between two vehicles is uploaded to Cloud [3] via existing cellular technologies, e.g., 3G or LTE. After collecting these social connections, a social network among vehicles could be built and downloaded by vehicles. In the distributed solution, each vehicle shares its social connections with nearby vehicles via DSRC technology. By exchanging social connections with others, a vehicle can incrementally construct its vehicular social network. Although the centralized one provides a reliable and real-time solution, the distributed one is cheaper as it has no dependence on infrastructures. We believe these two solutions are complementary to each other, i.e., when cloud service is not available or too expensive, a distributed solution becomes a better candidate, and vice versa.

A social connection in VSN initiates when two vehicles encounter and share information with each other. Such connection information will be either uploaded to Cloud [4] or saved by these two vehicles. In this article, we focus on constructing VSNs in a distributed manner as it is a cheaper solution requiring no infrastructures. In the distributed solution, each vehicle maintains a local social connection tree (SCT). The root of a local SCT is the vehicle that maintains this SCT, the edges in the SCT are the (direct or indirect) social connections of the vehicle.

As shown in Fig. 2, a vehicle (e.g., n_0) keeps tracking the interactions between itself and nearby vehicles. If it receives a message, e.g., road condition from vehicle n_2, it first checks whether n_2 is in its local SCT. If not, a node n_2 is created and inserted into its local SCT. Otherwise, the weight of the edge between n_0 and n_2 is updated based on the new interaction. The more the positive interactions, the stronger (heavier) the connection (edge).

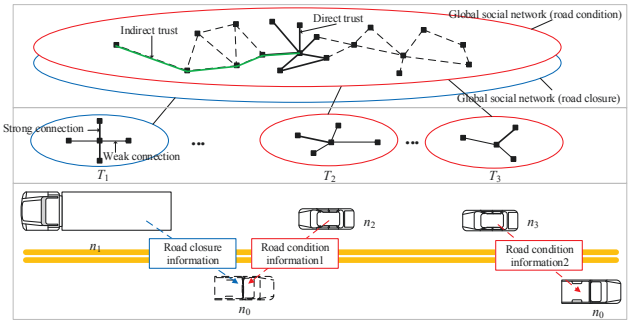

Fig. 2. Illustration of a distributed vehicular social network construction

When two vehicles encounter each other on the road, they could also share their local SCTs. With the SCTs received from others, a vehicle can incrementally build its global social network. Knowing more vehicles with the common interests and receiving more relevant information motivates vehicles to share its local SCT with others. Both local SCTs and global social networks are built in a distributed manner, so the constructing process scales in large-size vehicular networks.

If a social network structure exists in a vehicular network, it is possible to study the trustworthiness among vehicles by a social network approach. For example, if two vehicles have a weak connection, it probably means the trustworthiness between them is low. At least, there is a lack of positive evidences indicating a trustful connection between them. Later on, if they exchange lots of useful information, the weak connection may become a strong one, indicating high trustworthiness between them.

The trust computed from vehicle interactions is considered direct trust as vehicles are directly connected to each other. Another type of trust is called indirect trust, which describes the trust relations of vehicles that never physically meet. For example, a vehicle may have virtual connections to vehicles recommended by its "friends."

Last but not the least, trust is context-specific, so different local SCTs and global social networks are needed for different contexts. For instance, when vehicle n_0 receives road closure information from truck n_1, the connection between n_0 and n_1 is created in n_0's local SCT dedicated to road closure. Later on, when it receives local SCTs about road conditions from n_2 and n_3, these SCTs are integrated into n_0's global road-condition social network. How to classify messages into different categories is a tradeoff issue where more categories (contexts) increase the processing time and storage while fewer categories yield inaccurate trust estimations.

III. Trustworthy Vehicular Social Networks

Thanks to the technological advances of wireless networks, drivers in populated locales are connected to form a tightly-coupled and ad-hoc mobile vehicular social network (VSN). Within such a mobile social network, trustworthiness between temporarily connected vehicles could be mined from their interactions and applied within a VSN to achieve trustworthy information sharing among vehicles [5]. In this section, we start with the current research on direct and indirect trust in OSN and then extend them to VSN. Finally, we will provide a discussion on what the authors believe are the most important research challenges that lie ahead.

A. Direct Trust Measurement

Several works about direct trust measurement in online social networks exist. Researchers focused on measuring trustworthiness in OSN based on users' similarity [6] and interactions [7].

1) Direct Trust in OSN: Strong correlation between trust and users' interest similarity was found in [6], based on the data obtained from two real-world online communities – All Consuming and FilmTrust. For each dataset, a user's interest profile is constructed from the ratings he made on corresponding items, e.g., books or movies. Such interest profiles are then used to compute the similarities between different users. The trust level between any two users is then measured from the profile similarity. In other words, the more similar the users, the more likely they trust each other.

Besides user interest similarity, direct trust can also be mined from user interactions. In [7], the authors asked 35 participants to rate the trustworthiness of their Facebook friends, which served as the ground truth. 74 Facebook variables were then collected for each participant and used to compute the trustworthiness of his friends. Finally, the authors model tie/connection strength between users as a linear combination of these predictive variables. They discover user interaction data can be used to distinguish strong and weak ties with more than 85% accuracy.

2) Direct Trust in VSN: Previous study on direct trust in ONS reveals that it is possible to compute or mine direct trust from driver interest similarities and interactions in VSNs. To apply the existing approaches, however, we need to make some modifications. For example, the user interest similarity between vehicles should be re-defined because the only product in VSNs are messages exchanged between vehicles. Information shared between vehicles should be classified into different categories as that in [6], and a driver's interest profile vector should be built from ratings of all categories. The rating of a category can be modeled as the user's estimate about the trustworthiness of received information in that category. To determine whether a received message is trustworthy or not, each vehicle must have an information discrimination system. Vehicles could rely on their own sensors to evaluate the trustworthiness of received messages. In addition, they can upload received messages to Cloud to conduct information discrimination.

If information sharing between vehicles are considered as the interactions between drivers, mining trust from interacting data becomes a suitable solution to obtaining direct trust between vehicles. However, messages are exchanged only when two vehicles with a common interest encounter each other, so research are needed to study how such interactions can reflect trust between vehicles. Besides, compared to OSN, the volume of vehicular interaction data could be extremely large because vehicles can potentially exchange messages with all neighboring vehicles. Therefore, a resource-aware information discrimination scheme is needed so that only the most relevant information is shared between vehicles with a common or similar interest.

B. Indirect Trust Inference

Due to the propagative nature of trust, focus of indirect trust inference mainly lies in modeling trust propagation along trust relations between people who do not have direct trust connections [8]. To model and determine the trust between two users having no direct interaction in OSN, there are mainly two types of method in the literature: topology-based and evidence-based methods.

1) Indirect Trust in OSN: A good example of topology-based method is proposed in [9], which leverages the truth that a disproportionately-small "cut" exists between Sybil, users with multiple fake identities, and honest nodes to distinguish distrustful from trustful users. Since this approach is designed to identify Sybil users, indirect trust is considered a binary value indicating whether a user is trustful or not.

The authors discover that a distrustful user may create many fake identities but could build a limited number of connections (or edges) to legitimate users. By looking at the

social connections between users, the community composed of distrustful nodes can be identified and eliminated from the trustful ones. Topology-based indirect trust inference is good for some applications, e.g., Sybil node detection, but it has limitations in computing non-binary trustworthiness, which could be addressed by the evidence based approaches [10].

To understand indirect trust in online social networks, Jøsang proposed the seminal work of modeling trust by the subjective logic model [10]. Subjective logic is a type of probabilistic logic based on the Dempster-Shafer belief theory, it explicitly takes uncertainty and belief ownership into account while computing trustworthiness. It treats trustworthiness as opinions and introduces an algebra for opinion operations, e.g., discounting and consensus operations. An opinion in the subjective logic contains three components: belief, distrust and uncertainty; which reflect the subjectivity and uncertainty existing in user's assessment of others' trustworthiness.

2) Indirect Trust in VSN: While direct trust could be obtained from vehicles' similarity and interactions, indirect trust is derived from other vehicles' recommendations. The indirect trust from a trustor vehicle to a trustee vehicle highly depends on how strongly they are connected, which is affected by many factors such as the social distance, connection strengths and social network topology between them. If the trustworthiness of all connections in a vehicle's global social network are known, the problem of computing indirect trustworthiness in VSN can be defined as follows.

Given the global social network $G(V, E)$ of a certain vehicle u, $\forall$ vehicle v such that $e(u, v) \notin E$, and $\exists$ at least one path from u to v, how to compute the trustworthiness of v to u, i.e., how u should trust a stranger v based on his social connections.

To solve this problem, the evidence-based approach is more appropriate than the topology-based ones because subjective logic is able to compute non-binary trust values, which enables the comparison between trustful vehicles, e.g., to identify the most trustful vehicle. Moreover, non-binary trust values also mean more accurate trust evaluations.

Applying subjective logic to compute indirect trust in VSN, however, faces a few challenges. First, the subjective logic defines trust as an opinion vector containing *belief*, *distrust* and *uncertainty*. Most existing direct trust datasets only provide the values of belief, e.g., the trust level of a relation is 0.7. The other 0.3, however, could mean either distrust, uncertainty, or both. Second, subjective logic could not handle complex topologies. Although some approximation solutions are proposed to select the strongest path while computing indirect trust in a complex network, the selection procedure causes information loss in trustworthiness computation. Third, applying subjective logic on a graph requires finding all possible paths (social connections) between two vehicles, which is an NP-Hard problem. Therefore, procedures are needed to control the size of local SCTs on vehicles, to trim global social network by eliminating less trustful edges, and to design an approximation algorithm to find all paths between the trustor and trustee vehicles.

In summary, a vehicle could evaluate the direct trust of another vehicle based on their past interactions, and infer indirect trust by investigating how closely they are socially connected. This approach is different from traditional ones that focus on securing or authenticating vehicles based on the public key infrastructure (PKI). While PKI builds the first line of defense, it guarantees only the identification of legitimate vehicles but not the trustworthiness of vehicles.

IV. Research Challenges

There are many challenges in deploying a trustworthy vehicular social network, e.g., increasing the penetration rate of equipped vehicles, constructing adequate roadside infrastructure, and establishing new policies and laws. In this article, however, we only focus on the technical issues relevant to designing a trustworthy vehicular network. To realize a trustworthy VSN, the following research challenges need to be addressed: (1) information classification and discrimination, (2) resource-aware information discrimination, (3) appropriate indirect trust model, and (4) efficient algorithm for computing indirect trust.

A. Information Classification and Discrimination

To achieve context-aware trust evaluation, messages exchanged among vehicles must be classified into different categories and discriminated based on their trustworthiness. On each vehicle, a trust evaluation system will be developed to affirm the information conveyed in received messages. Vehicles could rely on their own on-board sensors and roadside infrastructures to obtain the ground truth and then discriminate the trustworthiness of received messages. Such a system will enable a vehicle to distinguish positive from negative and uncertain messages. With the subjective logic model [10], trustworthiness between vehicles could be modeled based on the amount and nature (positive, negative or uncertain) of their interactions.

Furthermore, this trust evaluation system should encompass the multifaceted (e.g., dynamic, asymmetric, and subjective) aspects of trust. Analyzing messages exchanged among vehicles might cause the privacy leakage of drivers, so privacy protection mechanisms are also needed.

B. Resource-Aware Information Discrimination

With the basic trust evaluation system being set up, it is essential to study resource-aware information discrimination due to the massive amount of messages exchanged between vehicles. For example, a probabilistic information discrimination mechanism might help a vehicle spend its resource on discriminating the messages with the greatest application relevance. In addition, a piggybacked notification scheme could reduce the communication overhead by sending the notification of untrustworthy vehicles to others. With this scheme, vehicles that are unable to identify untrustworthy messages will learn of such information from their trustworthy "friends".

C. Indirect Trust Model

A VSN can be considered a dynamic graph where nodes represent vehicles and time-varying edges indicate connections between temporarily connected vehicles. Given such

a dynamic graph, the following research questions need to be studied. Does indirect trust exist between vehicles? Is it possible to compute the indirect trust between vehicles from their social connections? How to appropriately model trust propagation within VSNs? Could multiple trust relations be combined to form a new one (and how)? What is the best way to compute the expected trustworthiness of a social connection?

D. Efficient Algorithm on Computing Trust

Assuming the indirect trust model is in place, an efficient indirect trust computation algorithm is needed. This is because finding all possible paths between two vehicles in a global social network is NP-Hard. Therefore, a global social network must be pre-processed, e.g., divided into disjoint clusters with small diameters, so searching all paths only occurs within a cluster. Existing clustering algorithms, e.g., k-means algorithm and spectral analysis, can be applied to split a global social network into several smaller clusters.

As shown in Fig. 3, a global social network is divided into 4 clusters and only a sub-graph (e.g., cluster C_1) is used to compute the trustworthiness between nodes u and v. If these two nodes are not in the same cluster, e.g., u and v', the original network (composed of clusters $C_1 - C_4$) will be used.

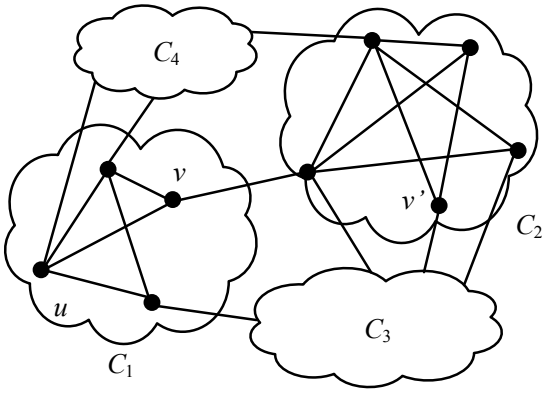

Fig. 3. A trust social network is split into different clusters (or clubs)

Alternatively, we can dynamically adjust the algorithm's searching depth, i.e., if the computed indirect trust between the trustor and trustee is accurate, there is no need to search deeper to find all possible paths.

V. Conclusion

This article has provided a social network approach to study trustworthy vehicular networks, i.e., measuring direct trust from past interacting data and infer indirect trust from social recommendations among vehicles. The evolution of social connections between vehicles and the construction of vehicular social network are first investigated, followed by an overview of the progress in research of direct and indirect trust in online social networks. Although there are similarities between a vehicular social network and its analogues, online social networks, there appears to be a divide between these two fields.

Leveraging results for online social networks, many new research opportunities exist in trustworthy VSN, e.g., VSN construction protocol, message classification and discrimination, trust information discrimination, privacy protection, direct trust measurement, indirect trust inference, trust computing algorithm, simulation and experiment platforms, and VSN dataset containing trust information. With the increasing deployment of connected vehicles, the authors expect to see more interdisciplinary research efforts devoted to studying trustworthy VSNs.

References

[1] "Connected car market (2013-2018)," 2013, [Online; accessed 19-Sep-2014].

[2] S. Smaldone, L. Han, P. Shankar, and L. Iftode, "Roadspeak: Enabling voice chat on roadways using vehicular social networks," in *Proceedings of the 1st Workshop on Social Network Systems*, 2008, pp. 43–48.

[3] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud-based vehicular networks with efficient resource management," *IEEE Network*, vol. 27, no. 5, pp. 48–55, September 2013.

[4] G. Nan, Z. Mao, M. Li, Y. Zhang, S. Gjessing, H. Wang, and M. Guizani, "Distributed resource allocation in cloud-based wireless multimedia social networks," *IEEE Network*, vol. 28, no. 4, pp. 74–80, July 2014.

[5] D. Huang, X. Hong, and M. Gerla, "Situation-aware trust architecture for vehicular networks," *Communications Magazine, IEEE*, vol. 48, no. 11, pp. 128–135, November 2010.

[6] C.-N. Ziegler and J. Golbeck, "Investigating interactions of trust and interest similarity," *Decis. Support Syst.*, vol. 43, no. 2, pp. 460–475, 2007.

[7] E. Gilbert and K. Karahalios, "Predicting tie strength with social media," in *CHI '09*, 2009, pp. 211–220.

[8] G. Liu, Q. Yang, H. Wang, X. Lin, and M. Wittie, "Assessment of multi-hop interpersonal trust in social networks by three-valued subjective logic," in *INFOCOM, 2014 Proceedings IEEE*, April 2014, pp. 1698–1706.

[9] H. Yu, M. Kaminsky, P. B. Gibbons, and A. D. Flaxman, "Sybilguard: Defending against sybil attacks via social networks," *IEEE/ACM Trans. Netw.*, vol. 16, no. 3, pp. 576–589, 2008.

[10] A. Jøsang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 9, no. 03, pp. 279–311, 2001.