A hybrid trust model based on communication and social trust for vehicular social networks

Na Fan¹, Shuai Shen¹, Chase Q Wu² and Junfeng Yao¹

Abstract
Vehicular social networks are emerging hybrid networks that combine traditional vehicular networks and social networks, with two key types of nodes, that is, vehicles and drivers. Since vehicle behaviors are controlled or influenced by drivers, the trustworthiness of a vehicle node is essentially determined by its own communication behaviors and its driver’s social characteristics. Therefore, human factors should be considered in securing the communication in vehicular social networks. In this article, we propose a hybrid trust model that considers both communication trust and social trust. Within the proposed scheme, we first construct a communication trust model to quantify the trust value based on the interactions between vehicle nodes, and then develop a social trust model to measure the social trust based on the social characteristics of vehicle drivers. Based on these two trust models, we compute the combined trust assessment of a vehicle node in vehicular social networks. Extensive simulations show that the proposed hybrid trust model improves the accuracy in evaluating the trustworthiness of vehicle nodes and the efficiency of communication in vehicular social networks.

Keywords
Vehicular social networks, hybrid trust model, communication trust, social characteristics, social trust

Date received: 31 August 2021; accepted: 3 March 2022

Handling Editor: Yanjiao Chen

Introduction
In recent years, with the rapid development and wide use of Internet of things (IoTs), vehicular social networks (VSNs) have emerged as a new type of communication network that combines both traditional vehicular wireless networks and social networks. VSNs contain two key types of entities, that is, vehicles and drivers, and provide a reliable and manageable communication system to meet both safety requirements and socialization needs.

An increasing number of applications have been developed based on VSNs for various purposes such as safety improvement, traffic management, urban sensing, and multimedia sharing. Some vehicular social-based applications exploit widely used social networking services, such as Facebook and Twitter, to provide a foundation of social relations for users with common interests. For example, Ford developed Twittermobile car, which is able to send and receive Twitter messages, containing information ranging from the driver’s mood (status) to real-time traffic warnings. Similarly, Navitweet is used to post or listen to traffic information, so that the driver’s preferences can be incorporated into the navigator’s route calculation.¹ RoadSpeak is a

¹School of Information Engineering, Chang’an University, Xi’an, China
²Department of Computer Science, New Jersey Institute of Technology, Newark, NJ, USA

Corresponding author:
Na Fan, School of Information Engineering, Chang’an University, Middle Section of Nan’er Huan Road, Xi’an 710064, Shaanxi, China.
Email: fnsea@chd.edu.cn

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
Voice chatting system used by daily commuters or a group of people who are on a commuter bus or train.\(^2\) Waze is a free social mobile app that enables drivers to build and use live maps with real-time traffic updates and turn-by-turn navigation.\(^3\) In such applications, vehicles and drivers are related to each other and their social characteristics could be utilized to facilitate the development of more efficient vehicular networks.

VSNs are constructed based on the social connections between drivers or communication links between vehicles. Analyzing VSNs can help us monitor the evolution of traffic, identify social groups with similar trajectories, and predict traffic conditions such as rush hours. For instance, intelligent traffic management helps adjust travel schedules to reduce the negative impact of traffic on our daily lives. Particularly, with real-time data collected from VSNs, it is possible to generate a live traffic map that shows the volume of traffic at different locations and share such information among drivers to avoid congested roads. Also, different drivers sharing the same trip may discuss topics of common interests and exchange various messages such as traffic jam, road construction, and car incident. Many vehicular applications not only use cryptographic techniques for data protection, but also require a level of confidence on accepting messages from other neighbor nodes. However, providing such confidence is difficult because it is more challenging to evaluate the trustworthiness of vehicles and drivers in vehicular ad hoc networks with short-lived connections than other communication networks with a relatively stable group of users. Most existing methods use historical communications between nodes to evaluate the trustworthiness of vehicular nodes,\(^4\)\(^-\)\(^7\) and social characteristics of drivers still remain largely unexplored. However, human factors, such as personalities, moods, and user preferences, oftentimes play an important role in driving behavior and vehicular communication, and hence should be considered in evaluating the trustworthiness of vehicular nodes.

In this article, we extend the previous work by Fan and Wu\(^8\) to develop a hybrid trust scheme for VSNs. In the work by Fan and Wu,\(^8\) we constructed a trust model to evaluate vehicular nodes. The communication behavior of vehicular nodes was considered in the model. However, human factor, such as social relationship among vehicular nodes, was not taken into account in the model. In this article, we take into account human factors and analyze the influence from social relationships between drivers. This hybrid scheme evaluates the trustworthiness of a vehicular node based on both communication trust and social trust. Particularly, in the model of social trust, we identify and extract social characteristics from the social relationships between drivers. In addition, similar to traditional networks, VSNs are also challenged with cybersecurity threats such as black hole attack and on–off attack. The social information incorporated in our scheme helps build a more efficient way to defend against these cyber attacks in VSNs.

To the best of our knowledge, we are among the first to exploit the social characteristics of drivers from social networks in evaluating the trustworthiness of vehicle nodes. This work makes the following technical contributions to the field:

- We propose a hybrid trust scheme to evaluate the trustworthiness of a vehicle node based on a combination of both communication trust and social trust in VSNs.
- We construct a social trust model based on drivers’ social characteristics for calculating the social trust assessment of drivers in VSNs.
- We develop a new secure protocol based on the proposed hybrid trust scheme to improve the efficiency of message transfer and defend against black hole attack and on–off attack.

The rest of the article is organized as follows. In section “Related work,” we conduct a survey of related work on the trustworthiness evaluation of vehicular nodes and social characteristics mining. In section “Network model and problem statement,” we construct a VSN model and formulate the problem. Section “Hybrid trust model for evaluating vehicular nodes” details the design of a hybrid trust model. Section “Simulation-based experiments and performance evaluation” presents and analyzes the experimental results for performance evaluation. Finally, we provide a summary of our work and sketch a plan of future research.

Related work

In this section, we shall start with a brief introduction to existing efforts in evaluating the trust level of vehicular nodes. Social characteristics in VSNs and existing research on social trust are also described.

Evaluating trustworthiness of vehicular nodes

The trust level of vehicular nodes has an impact on the efficiency of vehicular networks. Evaluating the trustworthiness of vehicular nodes is a key part of the trust scheme for vehicular networks, which has been extensively studied in the literature.

Generally, the methods for evaluating the trustworthiness of a vehicular node fall into three categories. The first category is to calculate a direct trust value based on the direct communications between neighbor nodes. For example, Gazdar et al.\(^9\) proposed a distributed trust computing framework based on an
investigation into the direct communication experience between neighbor vehicles. Based on this framework, they designed a tier-based message dissemination technique to detect eavesdropped messages and fake events. However, the direct trust method cannot be used if some vehicular nodes have never interacted with each other. These cases are not rare because vehicular networks are of dynamic and temporary characteristics.

The second category is based on indirect trust or recommended trust. If a vehicular node \( V_i \) has never communicated with another node \( V_j \), it may check with its neighbors that have communication behaviors with \( V_j \) to help compute a trust value about \( V_j \). The methods in this category have been widely used as a supplementary approach in various trust models when a direct trust value cannot be obtained, but typically are not used alone due to the accuracy issue.

The third category of methods are based on a hybrid model, which combines direct and indirect trust values with different weights to evaluate the trustworthiness of a node. Krishna et al.\(^{10}\) designed algorithms to estimate the trustworthiness of nodes in Vehicular ad hoc networks (VANETs) with the help of a consensus mechanism. Kerrache et al.\(^{11}\) developed a hierarchical trust establishment solution based on a three-level architecture. Yao et al.\(^{12}\) constructed a dynamic entity-centric trust model based on weights according to the types of applications and the authority levels of nodes. Kerrache et al.\(^{13}\) proposed a trust establishment architecture, T-VNets, to estimate traffic density, trust among entities, and dishonest node distribution. In addition, by combining different trust metrics such as direct, indirect, event-based and Road Side Unit (RSU)-based trust, T-VNets is able to eliminate dishonest nodes from all network operations while selecting the best paths to deliver legitimate messages by taking advantage of the concept of link duration. Li and Song\(^{14}\) designed an attack-resistant trust management scheme (ART) for VANETs, where the trustworthiness of both data and mobile nodes is evaluated and used to detect and mitigate malicious attacks. Minhas et al.\(^{15}\) introduced a multi-faceted trust model that adopts a recommended trust value. Lu et al.\(^{16}\) proposed a blockchain-based anonymous reputation system, where a trust model is constructed to improve the trustworthiness evaluation of messages considering the reputation of the sender based on both direct historical interactions and indirect opinions about the sender. In the work by Cheng et al.\(^{6}\) a three-valued subjective logic model is proposed to evaluate trust between vehicles, and a trust assessment scheme is designed in VSNs. The proposed solution enables objective and subjective trust assessment of vehicles. In a previous work, Kerrache et al.\(^{17}\) designed a trust-based framework based on a developed intrusion detection module (IDM) and data-centric verification. In the work by Kerrache et al.,\(^{18}\) a trust-based scheme was proposed that adopted threshold adaptive control technique to detect intelligent malicious behaviors. In the work by Kerrache et al.,\(^{19}\) a risk-aware trust-based architecture was proposed to evaluate the trust among vehicles.

The aforementioned methods rely on only communication behaviors between vehicle nodes without taking into account human factors, especially the social relationships between drivers.

Social characteristics and social trust

Vehicles are driven by humans with their individual decision-making capability and driving behavior. Hence, the motion and communication of vehicles are inevitably affected by human factors, including social standing and user personalities and preferences. In recent years, with the rapid development of VSNs, significant efforts have been devoted to mining the social relationships between vehicle nodes and constructing suitable trust schemes in VSNs.

There exists some work on social characteristics mining in vehicular networks. Alishve et al.\(^{20}\) introduced social energy, which is defined to depict energy generated when two particles collide. Such characteristics are used to design social-based routing approaches in mobile social delay-tolerant networks (DTNs). Li et al.\(^{21}\) proposed space–time approachability and social approachability to depict the probability of a vehicle approaching the destination, which is used in a data-forwarding algorithm. Zhang et al.\(^{22}\) proposed an INterest-BAsed Routing (INBAR) framework for VSNs, where a new metric of community energy as a social characteristic is developed to indicate nodes’ social proximity to make forwarding decisions. Mantas et al.\(^{23}\) extracted the social relationships of the owner of a node from online social media and selected next forwarding nodes based on their social relationships. Yang and Wang\(^{24}\) proposed a social network approach for trustworthy information sharing in vehicular networks, which uses direct trust to mine driver interest similarities and interactions, and measures indirect trust by investigating how closely drivers are socially connected. Gu et al.\(^{25}\) designed a social-aware routing algorithm based on fuzzy logic algorithm to improve data packet delivery and reduce end-to-end delay. In this algorithm, several social attributions of nodes are considered, such as social centrality, similarity of nodes, and social activeness. However, the aforementioned methods do not consider the relationship between social characteristics of drivers and communication history of vehicular nodes.

With the mining of social characteristics, some methods that focus on calculating social trust in VSNs have been proposed. The work by Al-Qurishi et al.\(^{26}\) proposed SybilTrap, which uses a semi-supervised technique to automatically integrate the underlying features
of user activities with the social structure into one system. This method can effectively assist in the defense of Sybil attacks, but cannot be directly used in vehicular networks. Li et al.\textsuperscript{27} used social trust based on distance and similarity to improve cooperative communication quality. Zhu\textsuperscript{28} proposed a trustworthy group trust metric for P2P service sharing (TMPSS) economy based on personal social network (PSN) of users. This method considers various factors such as social circle similarity, preference similarity, interaction degree, and node reliability and produces an ordered set of reliable nodes to prevent activities of unreliable nodes. Wu et al.\textsuperscript{29} proposed an on–off attack–resistant data forwarding mechanism (OADM) for mobile social networks (MSNs) to detect an on–off attack based on the trust evaluation of nodes. Zhang et al.\textsuperscript{30} proposed a multi-criteria detection scheme of collusive fraud organization to address the collusive fraud problem in social networks, using node trust evaluation based on node communication. Liu et al.\textsuperscript{31} proposed a trust management scheme based on a cloud model, which adopts a specific computation operator to transform from qualitative concepts to quantitative computation. Chen et al.\textsuperscript{32} designed a dynamic trust management scheme in DTN environments in the presence of well-behaved, selfish, and malicious nodes, using a weighted voting method to minimize trust bias and identify malicious nodes. Raj and Balasubramanian\textsuperscript{33} designed a similarity-based trustworthy routing algorithm, which incorporates social features into trustworthy routing. It evaluates the social features of vehicular nodes and selects the best node for forwarding. However, these aforementioned methods were designed for traditional social networks and cannot be directly used in VSNs. However, aforementioned methods were designed for traditional social network and cannot be directly used in VSNs.

Table 1 summarizes the main existing works for vehicular networks.

| Cites | Communication trust | Social trust | Resist attacks |
|-------|---------------------|--------------|---------------|
|       | Direct trust | Indirect trust | Road side units Trust | Single factor | Multiple factors | |
| Gazdar et al.\textsuperscript{9} | ✓ | | ✓ | | | |
| Krishna et al.\textsuperscript{10} | ✓ | ✓ | | | | |
| Kerrache et al.\textsuperscript{11} | ✓ | ✓ | ✓ | | | |
| Yao et al.\textsuperscript{12} | ✓ | ✓ | ✓ | | | |
| Kerrache et al.\textsuperscript{13} | ✓ | ✓ | ✓ | | | |
| Li and Song\textsuperscript{14} | ✓ | | ✓ | | | |
| Minhas et al.\textsuperscript{15} | ✓ | | ✓ | | | |
| Lu et al.\textsuperscript{16} | ✓ | | ✓ | | | |
| Cheng et al.\textsuperscript{6} | ✓ | ✓ | | | | |
| Kerrache et al.\textsuperscript{17} | ✓ | ✓ | | | | |
| Kerrache et al.\textsuperscript{18} | ✓ | ✓ | | | | |
| Kerrache et al.\textsuperscript{19} | ✓ | ✓ | | | | |
| Alishelv et al.\textsuperscript{20} | ✓ | ✓ | | | | |
| Li et al.\textsuperscript{21} | ✓ | ✓ | | | | |
| Zhang et al.\textsuperscript{22} | ✓ | ✓ | | | | |
| Mantas et al.\textsuperscript{23} | ✓ | ✓ | | | | |
| Yang and Wang\textsuperscript{24} | ✓ | ✓ | | | | |
| Gu et al.\textsuperscript{25} | ✓ | ✓ | | | | |
| Al-Qurishi et al.\textsuperscript{26} | ✓ | ✓ | | | | |
| Li et al.\textsuperscript{27} | ✓ | ✓ | | | | |
| Zhu\textsuperscript{28} | ✓ | ✓ | | | | |
| Wu et al.\textsuperscript{29} | ✓ | ✓ | | | | |
| Zhang et al.\textsuperscript{30} | ✓ | ✓ | | | | |
| Liu et al.\textsuperscript{31} | ✓ | ✓ | | | | |
| Chen et al.\textsuperscript{32} | ✓ | ✓ | | | | |
| Raj and Balasubramanian\textsuperscript{33} | ✓ | ✓ | | | | |
| Kerrache et al.\textsuperscript{34} | ✓ | ✓ | | | | |

4 International Journal of Distributed Sensor Networks
Different from the existing methods, we propose a hybrid trust scheme to analyze communication behaviors and mine social characteristics of vehicle nodes to achieve a more comprehensive evaluation of node trustworthiness. This scheme facilitates the identification of legitimate messages, resists black hole and on–off attacks, and improves the efficiency of message transfer in VSNs.

**Network model and problem statement**

In this section, we present the model for VSNs and define the problem under study.

**VSNs model**

VSNs comprised two key components, that is, (1) a vehicular ad hoc network that represents the physical layer, and (2) a social network framework on top of the physical vehicular network. VSNs contains two types of entities, that is, vehicles and drivers, and involves various relationships, such as communications between vehicular nodes, and social ties or relationships between drivers. Similar to vehicular networks, which are constantly evolving, VSNs are also of dynamic characteristics due to the movement of vehicle nodes and the change of social relationships between drivers. The architecture of a typical VSN is illustrated in Figure 1.

In general, VSNs are of two main types: centralized and distributed. In centralized VSNs, a social relationship between two vehicles is collected and transmitted to a central node such as a cloud service node. In distributed VSNs, each vehicle node shares its social information with nearby vehicles. By exchanging social relationships with others, a vehicle can incrementally construct its own VSN. Centralized VSNs provide a reliable, real-time solution, while distributed VSNs are cheaper as they do not rely on infrastructures. In practice, these two solutions are complementary to each other. If the cloud service is not available or too expensive, a distributed structure could be used; if there are reliability and real-time requirements, a centralized one would be preferred. Due to the sparse distribution of cloud service nodes, it would be difficult for cloud nodes to cover the whole network. Hence, the distributed architecture is more popular and is the focus of our work.

**Problem statement**

VSNs combine vehicular networks and social networks, including traditional V2V and V2I communication protocols, as well as human factors, for example, driver personality and preferences, relationships between people, all of which may affect vehicular communication and connectivity.

Generally, the following aspects should be considered when building VSNs: (1) identification of social communities based on common characteristics where nodes interact with other members; (2) trust management and evaluation to update node trust levels based on nodes’ behaviors, interactions, activities, and participation in communities.

In VSNs, the trustworthiness of a vehicular node depends on not only its own communication behavior but also its driver’s social trust. Drivers in VSNs are related to each other according to their social relationship and can significantly affect the communication behavior of vehicular nodes. If a driver is trustworthy, the vehicular node being driven is also very likely trustworthy, and vice versa. Hence, it is reasonable to take into account communication trust from the communication behavior of vehicle nodes and social trust from drivers in evaluating the trustworthiness of vehicle nodes.

How to evaluate social trust is a challenging problem. The complicate social relationship will be analyzed. To tackle the challenge, we consider two design goals in our scheme as follows. The first goal is to consider the human factor and mine the social trust based on analyzing relationship of drivers. The second goal is to construct a hybrid trust model based on both communication trust and social trust to improve the accuracy of trustworthiness evaluation of vehicular nodes.
Hybrid trust model for evaluating vehicular nodes

Drivers control and drive vehicles, and hence largely determine vehicular nodes’ communication behaviors. In general, if a driver tends to share and exchange information with other drivers, a vehicle driven by this driver is also active and cooperative in communication with other vehicles. If two drivers have a social relationship, such as being friends, having common interests, and so on, two vehicles driven by these two drivers are more likely to construct trustworthiness between them. Therefore, in order to comprehensively evaluate whether or not a vehicular node is trusted, we consider two factors: communication trust and social trust. Communication trust is evaluated based on the historical behavior of a vehicle node, and social trust is calculated based on the detection of a social tie between drivers.

To evaluate the trustworthiness of vehicular nodes, we propose a hybrid model considering both communication trust and social trust. We leverage the scheme proposed by Fan and Wu\(^8\) to quantify the communication trust of a vehicular node and focus our work in this article on quantifying social trust. We compute the hybrid trust of a vehicular node by combining both types of trust.

The process of identifying the trustworthiness of a vehicular node includes three phases: (1) communication trust information collection and evaluation based on the scheme by Fan and Wu\(^8\), (2) social trust collection and evaluation, and (3) combined trust information evaluation. To identify how honest and trustful a vehicular node is, we derive social trust based on a scalar estimation using the personal profile information of a vehicle driver, which includes the driver’s interactions with other drivers. Figure 2 provides a schematic workflow for trust derivation.

Social trust model based on social characteristics

In VSNs, social relationships are built between drivers and are used to increase the trustworthiness in information exchange. In this section, we divide drivers into different social communities, explore social relationships between drivers, and compute the social trust value of drivers.

Identifying social community. In VSNs, a driver node has various attributes, which can be described as interests, preferences, or requirements for services. We describe a driver node \(v_i\) as \(\{v_{i1}, v_{i2}, \ldots, v_{ig}, \ldots\}\), where \(v_{ig}\) denotes the \(g\)th attribute of \(v_i\). Note that in real-life VSNs, a group of drivers may have similar interests or preferences. For example, if two drivers share a common interest in football, they may drive to the same stadium to watch a football game. Hence, there is a high probability that they encounter each other because of similar interests. Based on the social similarity between them, drivers can be divided into different social communities.

First, we model the social network in VSNs as \(G = (V, E)\), where \(V = \{v_1, v_2, \ldots, v_n\}\) denotes the set of driver nodes and \(E\) denotes the set of edges, each of which describes a certain type of social relationship between two nodes.

Then, we classify the driver nodes into different social communities. A community is defined as a subgraph, which consists of a group of nodes with strong connections. We employ an agglomerative clustering-based method to detect social communities. In VSNs, a driver node with several different interests may belong to more than one social community, and these are therefore termed overlapping communities, as illustrated in Figure 3, where \(v_k, v_q,\) and \(v_l\) are members of both communities \(C_p\) and \(C_q\). To address the overlapping problem, we design a social community division method by leveraging the Q-Modularity algorithm in Newman\(^37\) referred to as SCDQ, as detailed below.

1. For each driver node in \(V\), we calculate its degree centrality as follows

\[
DC_{vi} = \frac{\sum_{j=1}^{n} E_{vi,vj}(i \neq j)}{n - 1}
\]

where \(DC_{vi}\) denotes the degree centrality of node \(v_i\), and \(E_{vi,vj}\) denotes the number of edges between \(v_i\) and \(v_j\).

2. We calculate the similarity between two nodes \(v_i\) and \(v_j\) as follows
where $Sim_{v_i,v_j}$ denotes the similarity value between $v_i$ and $v_j$, and $D_{v_i,v_j}$ denotes the distance between $v_i$ and $v_j$, which is calculated as follows:

$$D_{v_i,v_j} = \sqrt{\sum_{k=1}^{g} (v_{ik} - v_{jk})^2} \quad (3)$$

where $g$ denotes the number of attributes of a node.

3. We calculate the average similarity value $AveSim$ as follows

$$AveSim = \frac{\sum_{k=1}^{g} (v_{ik} - v_{jk})^2}{g} \quad (4)$$

which is used as the threshold $W$ for dividing clusters.

4. According to the result of Step (1), we choose the node with the largest degree centrality as the center of clustering.

5. We assign any other node to the cluster if its similarity with the cluster center is larger than the threshold $W$, and remove it from $V$.

6. If $V$ is not NULL, go back to Step (4); otherwise, move to Step (7).

7. If a node is simultaneously divided into different clusters, the Q-Modularity algorithm is used to assign the node to the cluster where it has the largest modularity value.

The pseudocode of SCDQ is provided in Algorithm 1.

Based on the graph theory, the adjacency matrix $A$ of $G$ is defined as follows:

$$A_{v_i v_j} = \begin{cases} 1, & \text{one edge between } v_i \text{ and } v_j \\ 0, & \text{no edge between } v_i \text{ and } v_j \end{cases} \quad (5)$$

We calculate the total number edges of graph $G$ as follows

$$m = \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} A_{v_i v_j} \quad (6)$$

where $n$ denotes the total number of nodes in $V$.

We calculate the value of Q-Modularity of a cluster as follows

$$Q = \sum_{ij} \left[ \frac{A_{v_i v_j}}{2m} - \frac{DC_{v_i}DC_{v_j}}{(2m)^2} \right] \Psi(C_{v_i}, C_{v_j}) \quad (7)$$

where $Q$ denotes the modularity value of a cluster, $m$ is the number of edges in graph $G$, $DC_{v_i}$ and $DC_{v_j}$ are the centrality degrees of node $v_i$ and $v_j$, respectively, and $\Psi(C_{i}, C_{j})$ is 1 when $i = j$, and is 0, otherwise. The value of $Q$ indicates the strength level of inter-node social relationships in the social community: a larger $Q$ value of a community means stronger social relationships between nodes in the community.

The process of calculating the modularity values of a social cluster is described in Algorithm 2 [H].

According to the results of Algorithm 2, a node that is simultaneously divided into several clusters is assigned to only one cluster, which addresses the challenge brought by the overlapping problem.

**Social characteristics mining.** Drivers in VSNs may have various social characteristics, which are the basis for calculating social trust. In this section, we derive social relationships between drivers.

Generally, the lifespan of a social relationship is divided into three stages. Figure 4 shows the lifespan of a social tie.

**Creation of social relationship.** In this stage, a social relationship is constructed when two drivers connect with each other, exchanging and sharing various information.
Algorithm 1. SCDQ \((G, V, E)\).

\[
\begin{align*}
\text{Input:} & \text{ a graph } G; \text{ a set } V \text{ of driver nodes; a set } E \text{ of edges} \\
\text{Output:} & \text{ The results of social community set } C \\
1: & \text{ for all driver node } v_i \in V \text{ do} \\
2: & \text{ Calculate the degree value of node } v_i; \\
3: & \text{ Calculate the similarity value between node } v_i \text{ and other nodes;} \\
4: & \text{ end for} \\
5: & \text{ Calculate the average of similarity values } \text{Ave}_v; \\
6: & \text{ Choose the node with the largest degree value as the center of cluster } C; \\
7: & \text{ for all driver node } v_i \in V \text{ do} \\
8: & \text{ if the similarity value between } v_i \text{ and } C > \text{Ave}_v, \text{ then} \\
9: & \text{ Place } v_i \text{ in cluster } C \text{ and remove it from } V; \\
10: & \text{ else} \\
11: & \text{ Do nothing;} \\
12: & \text{ end if} \\
13: & \text{ end for} \\
14: & \text{ if } V! = \text{ NULL then} \\
15: & \text{ Go back to Line 6;} \\
16: & \text{ else} \\
17: & \text{ for all driver node } v_i \in C \text{ do} \\
18: & \text{ if node } v_i \text{ belongs to more than one cluster then} \\
19: & \text{ Call Q-Modularity;} \\
20: & \text{ Compare the modularity values;} \\
21: & \text{ Place } v_i \text{ in the cluster that has the largest modularity value;} \\
22: & \text{ Remove } v_i \text{ from other clusters;} \\
23: & \text{ else} \\
24: & \text{ Move to Line 21;} \\
25: & \text{ end if} \\
26: & \text{ end for} \\
27: & \text{ end if} \\
28: & \text{ Output the social community set } C.
\end{align*}
\]

Enhancement of social relationship. In VSNs, once a social relationship between two drivers is built, the communication behavior between them improves the social connection. For example, if two vehicles frequently encounter and their drivers share information with each other (e.g. parking in the same parking lot, having similar commute routes), their social connection becomes stronger.

Exhaustion of social relationship. In this stage, when two drivers do not connect and exchanges information for a long period of time, the social relationship becomes weaker over time.

How to depict the social relationship between nodes is a challenging problem. Some researchers explored the social interrelationship between nodes. In 1973, Kochemazov \(^38\) introduced the concept of social tie strength based on four components: the frequency of contact, the length or history of the relationship, the duration of contact, and the number of transactions. Some researchers extended these measures to seven components to evaluate tie strength, including Frequency, Intimacy/Closeness, Longevity, Reciprocity, Recency, Multiple social context, and Trust. \(^39\) According to various network conditions, different measures can be used.

In this article, considering the characteristics of VSNs, we provide several definitions to describe the social relationship between two drivers.

Definition 1

**Frequency**

It denotes the frequency of communication between two nodes over a period of time \(^40\) and is defined as follows

\[
F_{v_iv_j} = \frac{f_{v_iv_j}}{f_v - f_{v_iv_j}}
\]

where \(F_{v_iv_j}\) is the frequency of node \(v_i\) with respect to node \(v_j\), \(f_{v_iv_j}\) denotes the number of communications between node \(v_i\) and node \(v_j\), and \(f_v\) denotes the total number of communications of node \(v_i\) per unit time.

Definition 2

**Closeness**

It means the communication time of a node connecting with another node and is described as follows

\[
C_{v_iv_j} = \frac{t_{v_iv_j}}{t_v - t_{v_iv_j}}
\]

where \(C_{v_iv_j}\) is the closeness of node \(v_i\) to node \(v_j\), \(t_{v_iv_j}\) denotes the communication time between node \(v_i\) and node \(v_j\), and \(t_v\) means the total communication time of node \(v_i\) connecting with all nodes per unit time.

Definition 3

**Interest similarity**

It denotes the social interest similarity between two nodes. The trust level between any two drivers is measured from their profile similarity. In other words, the more similar the drivers are, the more likely they trust each other. The driver interest
similarity should be redefined to mine the trust level of drivers. We use the Jaccard similarity to calculate the interest similarity as follows

\[
S_{vi,vj} = \frac{|I_v \cap I_v|}{|I_v \cup I_v|} = \frac{|I_v \cap I_v|}{|I_v| + |I_v| - |I_v \cap I_v|}
\]  

(10)

where \(S_{vi,vj}\) is the similarity of social communication between node \(v_i\) and node \(v_j\). \(I_v = \{I_{v1}, I_{v2}, \ldots, I_{vz}\}\) denotes the social interest profile of node \(v_i\), \(z\) is the dimension of social interest profile and \(I_{vc} \in \{0,1\}\). When \(S_{vi,vj}\) is equal to 1, the social characteristics of these two nodes completely match; when \(S_{vi,vj}\) is equal to 0, none of the interest attributes between node \(v_i\) and node \(v_j\) match.

**Social trust calculation.** Social trust is related to the social relationships between nodes. If two driver nodes are in different social communities, it is less likely that they have an intimate social relationship. To describe the difference of social community labels between node \(v_i\) and node \(v_j\), we introduce a concept of distance of social community, defined as follows.

**Definition 4**

**Distance of social community**

It denotes the distance between two different social communities. A longer distance of social community indicates a weaker social relationship between two communities. Walk Trap is a classical model and can be used to evaluate the distance of two different social communities. First, we obtain the adjacency matrix \(A\) of \(G\) as mentioned above, and then calculate the probability transition matrix \(P\) as follows

\[
P = D^{-1}A
\]  

(11)

According to the above definition of \(P\), the distance \(R_{C_p,C_q}\) of two social communities \(C_p\) and \(C_q\) is calculated as follows

\[
R_{C_p,C_q} = \| D^{-1}P_{C_p}^\rho - D^{-1}P_{C_q}^\rho \| 
\]  

(12)

Equations (11) and (12) can be rewritten as follows

\[
R_{C_p,C_q} = \sqrt{\sum_{k=1}^{n} \left( \frac{(P_{C_k}^\rho - P_{C_k}^\rho) \cdot (P_{C_k}^\rho - P_{C_k}^\rho)}{d(k)} \right)^2}
\]  

(13)

where \(k\) denotes any destination node, \(d(k)\) denotes the degree of node \(k\), and \(\rho\) denotes step length. In our experiments, \(\rho\) is empirically set to be 4.

We calculate the social trust of driver nodes \(v_i\) and \(v_j\) as follows

\[
T_{Social(v_i,v_j)} = F_{v_i,v_j} + C_{v_i,v_j} + S_{v_i,v_j} + R_{C_p,C_q}
\]  

(14)

where \(T_{Social(v_i,v_j)}\) denotes the social trust between driver nodes \(v_i\) and \(v_j\). When nodes \(v_i\) and \(v_j\) belong to the same social community, \(R_{C_p,C_q}\) is 0; otherwise, \(R_{C_p,C_q}\) is non-zero.

The social relationships between driver nodes in VSNs change over time. Considering the lifespan of social relationship, we consider decay of social trust. If two nodes do not communicate with each other for a long period of time, the social tie life cycle between them changes from the enhancement phrase to the exhaustion phrase, and the strength level of their social relationship decays. Social trust is also recursive in nature, which means that the current social trust value is estimated based on the previous interactions/social trust value. We compute the social trust of node \(v_j\) on node \(v_i\) based on their interactions, as defined in equation (14). Considering the decay and recursive factors, we calculate social trust as follows

\[
T_{Social(v_i,v_j),\tau} + \Delta \tau = T_{Social(v_i,v_j),\tau} \times e^{-\frac{\Delta \tau}{\lambda}}
\]  

(15)

where \(T_{Social(v_i,v_j),\tau + \Delta \tau}\) denotes the social trust value at time \(\tau + \Delta \tau\), \(T_{Social(v_i,v_j),\tau}\) denotes the social trust value at time \(\tau\), and \(\lambda\) denotes the decay coefficient.

The process for calculating social trust is provided in Algorithm 3.

**Combined trust calculating**

We propose a hybrid trust scheme for trustworthiness evaluation based on social trust and communication trust and compute the combined trust of two nodes as follows

\[
T_{v_i,v_j} = \alpha \times T_{Social(v_i,v_j)} + \beta \times T_{Communication(i,j)}
\]  

(16)

where \(T_{v_i,v_j}\) denotes the combined trust of vehicular node \(v_j\) on node \(v_i\), \(T_{Communication(i,j)}\) denotes the communication trust between vehicle node \(i\) and node \(j\), and \(T_{Social(v_i,v_j)}\) denotes the social trust between driver nodes \(v_i\) and \(v_j\), driver nodes \(v_i\) and \(v_j\) are the drivers of vehicular nodes \(i\) and \(j\), respectively, \(\alpha\) and \(\beta\) are two weights, and \(\alpha + \beta = 1\). We use the method in the work by Fan and Wu\(^8\) to calculate the value of \(T_{Communication(i,j)}\), which considers both the direct and indirect trust values evaluated based on communication behaviors between vehicular nodes and RSUs.
Algorithm 3. Social trust \((G, E, V)\).

**Input:** the graph \(G\); a set \(V\) of driver nodes; a set \(E\) of edges between nodes  
**Output:** social trust  

1. Calculate Frequency \(F_{v_i v_j}\) based on the communication behaviors;  
2. Calculate \(C_{v_i v_j}\) based on the communication behaviors;  
3. Calculate \(S_{v_i v_j}\) between nodes \(v_i\) and \(v_j\);  
   - if nodes \(i\) and \(j\) belong to the communities of \(p\) and \(q\) separately then  
     - Calculate the distance between \(p\) and \(q\) which is called \(R_{C_p C_q}\);  
   - the value distance of social community equals to 0;  
4. Calculate social trust of \(T_{\text{Social}(v_i v_j)} = \Delta t\);  
5. Output the set of social trust values.

**Simulation-based experiments and performance evaluation**

**Simulation environment**

In our simulation experiments, we first use “Simulation of Urban Mobility” (SUMO) to produce accurate mobility traces. SUMO is an open-source, highly portable, microscopic, and continuous road traffic simulation package designed to handle road networks at a city scale. We then use the Opportunistic Network Environment (ONE) to conduct simulation-based experiments, where vehicle nodes perform simulated movements with the shortest-path map-based movement model based on the Helsinki city map of Finland. We repeat the simulation for 10 rounds and calculate the average performance.

The experiments follow the flowchart shown in Figure 5, and the parameters of the experiments are provided in Table 2.

**Experimental results**

We conduct two sets of simulations to evaluate (1) the performance of the social trust method and (2) the performance of the proposed hybrid trust model, as follows.

**Evaluating the social trust method.** In this section, we evaluate the performance of social trust computing in the detection of malicious nodes. We used the method proposed to compute social trust based on the Epinions data set (http://reality.media.mit.edu/), which is a classical social data set. The Epinions has 131,828 nodes (users) and 841,372 edges. The social interests of nodes are mined by analyzing edges among nodes in data set. The relationships between these nodes in Epinions fall into two categories: honest and malicious. We select 300 nodes for performance evaluation in comparison with the method of TPS\(^{41}\) which proposes the novel model to generate and evaluate trust inference within online Social Networks. We consider false-positive rate, precision rate, and recall rate as performance metrics, defined as follows

\[
\text{False positive} = \frac{\text{the \# of truly normal nodes detected}}{\text{the total \# of malicious nodes detected}} \quad (17)
\]

\[
\text{Precision rate} = \frac{\text{the \# of truly malicious nodes detected}}{\text{the \# of untrustworthy nodes}} \quad (18)
\]

\[
\text{Recall rate} = \frac{\text{the \# of truly malicious nodes detected}}{\text{the total \# of truly malicious nodes}} \quad (19)
\]

The false-positive curve for each method is plotted in Figure 6, which shows that our method (S-T) that considers the social relationship between nodes achieves better performance. Figures 7 and 8 show the comparison of precision rate and recall rate, respectively. The method proposed considers the multiple factors which include frequency, closeness, interest similarity, and distance of social community to accurately evaluate the social trust between two nodes. These results show that our method, which considers and computes social trust, improves detection performance.

**Evaluating the hybrid trust scheme.** We use the Reality data set\(^{42}\) to evaluate the performance of the hybrid trust scheme. In VSN, there are two layers of independent space: a virtual cyber space, which is composed of social relationships between drivers, and a physical vehicle space, which is composed of vehicle nodes. We select 94 user nodes in the Reality data set and randomly match their identities to 94 vehicle identities. Thus, every vehicle driver is represented by a user node within the used data set.

In the experiments, we consider two types of attack: black hole attack and on–off attack. In a black hole attack, a node refuses messages from its neighbors, while in an on–off attack, the behavior of a malicious
node is more deceptive. Sometimes, it acts like a normal node and participates in sending or forwarding messages, but at other times, it refuses to send or forward messages. In our experiments, we vary the percentage of malicious vehicles from 10% to 40%.

We compare the hybrid trust method with the methods of BTMS\textsuperscript{43} and WVM\textsuperscript{32} for performance evaluation. BTMS proposed a credible Bayesian-based trust management scheme, and WVM proposed a dynamic trust management model for determining trustworthiness in response to dynamically changing network conditions. Figures 9–11 show the comparison of false-positive rate, precision rate, and recall rate, respectively, of these three methods as the percentage of malicious nodes increases from 10% to 40%. These results show that the hybrid trust model consistently outperforms the other methods in comparison.

We further integrate our hybrid trust scheme into the routing algorithm of Prophet as a new routing approach, referred to as R-hybrid, which selects the node with the highest hybrid trust value as a relay node. We use the Prophet routing, Epidemic routing, INBAR\textsuperscript{22} and BEEINFO-D&S\textsuperscript{44} as baseline methods for comparison. INBAR is a new INBAR framework for VSNs, and BEEINFO-D&S is a set of forwarding schemes based on utilization of density and social ties.

We consider delivery rate, average delay, and overhead rate to evaluate the performance of R-hybrid and others. The performance comparison with 25% malicious nodes is shown in Figures 12–14, and the performance comparison with 40% malicious nodes is shown in Figures 15–17, respectively.

The proposed R-hybrid method achieves a higher delivery rate and a lower overhead than the other methods in comparison. The average latency of the proposed

| Name of parameter       | Setting of parameter     |
|-------------------------|--------------------------|
| Scenario size (m\textsuperscript{2}) | 3500 × 3500              |
| Movement model          | Shortest path map-based movement |
| Simulation time (s)     | 43800                    |
| Message generation interval (s) | 40 − 45              |
| Size of each message (KB) | 350 − 500           |
| Message survival time (min) | 350                |
| Delivery rate of node data (KB/S) | 250               |
| Node communication range (m) | 10                   |
| $\alpha$                | 0.4                     |
| $\beta$                 | 0.6                     |

\begin{table}[h]
\centering
\caption{Simulation parameters.}
\begin{tabular}{|l|l|}
\hline
Name of parameter       & Setting of parameter     \\
\hline
Scenario size (m\textsuperscript{2}) & 3500 × 3500              \\nMovement model          & Shortest path map-based movement \\
Simulation time (s)     & 43800                    \\nMessage generation interval (s) & 40 − 45              \\nSize of each message (KB) & 350 − 500           \\nMessage survival time (min) | 350                \\nDelivery rate of node data (KB/S) | 250               \\nNode communication range (m) | 10                   \\n$\alpha$                & 0.4                     \\n$\beta$                 & 0.6                     \\
\hline
\end{tabular}
\end{table}
method is affected by the communication behaviors of malicious nodes at the initial stage of VSNs because most of the nodes are not very active during that period. As the experiment proceeds with more communications occurring between vehicular nodes in VSNs, the proposed method based on the hybrid trust model is able to effectively resist the malicious nodes through the assessment of communication trust and social trust.

These experiment results show that compared with the other methods, the hybrid trust scheme provides better defense against black hole and on-off attacks and improves the efficiency of message transmission. Human factors are able to have important influence on evaluating trust of nodes in VSNs. In hybrid trust model, human factors are considered and social trust is computed based on human factors. Hybrid trust is
more accurate than communicate trust. R-hybrid considers both communication trust and social trust in selecting relay nodes, it effectively filters out malicious nodes and improves communication efficiency.

**Conclusion**

Trust establishment and evaluation in vehicle social networks is a challenging problem. In this article, we proposed a hybrid trust scheme for communication security in VSNs. We designed a social community division method based on social relationships between drivers to divide driver nodes into different communities. We also proposed new concepts to describe the social characteristics of nodes. We further developed a method of calculating social trust based on the social characteristics and the results of social community division. Within a hybrid trust scheme, we define a combined trust that combines both social trust and communication trust. Simulation results show that the hybrid trust model can effectively improve trust evaluation in VSNs.

In our future work, we plan to use and compare other data sets to evaluate our hybrid trust scheme. It is also of our interest to construct a combined platform, which combines both social networks and VANETs for experiments. In addition, considering the importance of privacy information, we plan to provide privacy protection for driver social information in our trust model.
Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research is supported by the Funding of Selected Science and Technology Projects of Oversea Scholars from Shaanxi Province (grant no. 20170723), the Fundamental Research Funds for the Central Universities (grant no. 300102240401), and the Shaanxi Provincial Key Scientific and Technological Project (grant no. 2020ZDLGY09-02).

ORCID iDs
Na Fan https://orcid.org/0000-0002-7431-6257
Chase Q Wu https://orcid.org/0000-0002-8218-1209

References
1. Sha W, Kwak D, Nath B, et al. Social vehicle navigation: integrating shared driving experience into vehicle navigation. In: Proceedings of the 14th HotMobile workshop on mobile computing systems and applications, Jekyll Island, GA, 26–27 February 2013, pp.161–166. New York: ACM.
2. Smaldone S, Han L, Shankar P, et al. RoadSpeak: enabling voice chat on roadways using vehicular social networks. In: Proceedings of the 1st workshop on social network systems, Glasgow, 1 April 2008, pp.43–48. New York: ACM.
3. Neto VR, Medeiros DSV and Campista MEM. Analysis of mobile user behavior in vehicular social networks. In: Proceedings of the international conference on the network of the future, London, 2017, pp.1–5, https://www.gta.ufrj.br/ftp/gta/TechReports/RMC16.pdf
4. Ahmad F, Hall J, Adnane A, et al. Faith in vehicles: a set of evaluation criteria for trust management in vehicular ad-hoc network. In: Proceedings of the IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData), Exeter, 21–23 June 2017, pp.44–52. New York: IEEE.
5. Ahmad S, Al-Rubeaai S and Tepe K. Novel trust framework for vehicular networks. IEEE Trans Veh Technol 2017; 66: 9498–9511.
6. Cheng T, Liu G, Yang Q, et al. Trust assessment in vehicular social network based on three-valued subjective logic. IEEE Trans Multim 2019; 21: 652–663.
7. Wan J, Gu X, Wang J, et al. A trust scheme based on vehicles reports of events in VANETs. Wirel Pers Commun 2019; 105: 121–143.
8. Fan N and Wu CQ. On trust models for communication security in vehicular ad-hoc networks. Ad Hoc Netw 2019; 90: 101740.
9. Gazdar T, Belghith A and Abutair H. An enhanced distributed trust computing protocol for VANETs. IEEE Access 2018; 6: 380–392.
10. Krishna TRV, Barnwal RP and Ghosh SK. CAT: consensus-assisted trust estimation of MDS-equipped collaborators in vehicular ad-hoc network. Veh Commun 2015; 2(3): 150–157.
11. Kerrache CA, Lagraa N, Calafate CT, et al. T-VNets: a novel trust architecture for vehicular networks using the standardized messaging services of ETSI ITS. Comput Commun 2016; 93: 68–83.
12. Yao X, Zhang X, Ning H, et al. Using trust model to ensure reliable data acquisition in VANETs. Ad Hoc Netw 2017; 55: 107–118.
13. Kerrache CA, Calafate CT, Lagraa N, et al. Hierarchical adaptive trust establishment solution for vehicular networks. In: Proceedings of the 2016 IEEE 27th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), Valencia, 4–8 September 2016, pp.1–6. New York: IEEE.
14. Li W and Song H. ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Trans Intell Transp Syst 2016; 17(4): 960–969.
15. Minhas UF, Zhang J, Tran T, et al. Intelligent agents in mobile vehicular ad-hoc networks: leveraging trust modeling based on direct experience with incentives for honesty. In: Proceedings of the IEEE/WIC/ACM international conference on web intelligence and intelligent agent technology, Toronto, ON, Canada, 31 August–3 September 2010, pp.243–247. New York: IEEE.
16. Lu Z, Wang Q, Qu G, et al. BARS: a blockchain-based anonymous reputation system for trust management in VANETS. In: Proceedings of the 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE), New York, 1–3 August 2018, pp.98–103. New York: IEEE.
17. Kerrache CA, Calafate CT, Lagraa N, et al. RTA: risk-aware trust-based architecture for collaborative multi-hop vehicular communications. Secur Commun Netw 2016; 9: 4428–4442.
18. Kerrache CA, Lakas A and Lagraa N. Detection of intelligent malicious and selfish nodes in VANET using threshold adaptive control. In: Proceedings of the 5th international conference on electronic devices, systems and applications, Ras Al Khaimah, United Arab Emirates, 6–8 December 2016, pp.1–4. New York: IEEE.
19. Kerrache CA, Lagraa N, Calafate CT, et al. TFDD: a trust-based framework for reliable data delivery and dos defense in VANETS. Veh Commun 2017; 9: 254–267.
20. Alishev D, Hussain R, Nawaz W, et al. Social-aware bootstrapping and trust establishing mechanism for vehicular social networks. In: Proceedings of the IEEE 85th vehicular technology conference, Sydney, NSW, Australia, 4–7 June 2017, pp.1–5. New York: IEEE.
21. Li Z, Wang C, Shao L, et al. Exploiting traveling information for data forwarding in community-characterized vehicular networks. IEEE Trans Veh Technol 2017; 66(7): 6324–6335.
22. Zhang C, Zhu L and Xu C. INBAR: a new interest-based routing framework in vehicular social networks. In: Proceedings of the international conference on security, pattern analysis, and cybernetics (SPAC), Shenzhen, China, 15–17 December 2017, pp.479–484. New York: IEEE.

23. Mantas N, Louta M, Katsaros K, et al. Social CLWPR: a socially enhanced position based routing protocol for handling misbehaviour in VANETs. In: Proceedings of the IEEE 8th international conference on information, intelligence, systems and applications (IISA), Larnaca, Cyprus, 27–30 August 2017, pp.1–6. New York: IEEE.

24. Yang Q and Wang H. Toward trustworthy vehicular social networks. IEEE Commun Mag 2015; 53(8): 42–47.

25. Gu X, Tang L and Han J. A social-aware routing protocol based on fuzzy logic in vehicular ad hoc networks. In: Proceedings of the international workshop on high mobility wireless communications, Beijing, China, 1–3 November 2014, pp.12–16. New York: IEEE.

26. Al-Qurishi M, Rahman SMM, Alamri A, et al. Sybil-Trap: a graph-based semi-supervised Sybil defense scheme for online social networks. Concurr Comput Pract Exp 2018; 30(5): e4276.

27. Li Y, Zhang Z, Wang H, et al. SERS: social-aware energy-efficient relay selection in D2D communications. IEEE Trans Veh Technol 2018; 67(6): 5331–5345.

28. Zhu W. A trustworthy group identifying trust metric for P2P service sharing economy based on personal social network of users. Wuhan Univ J Nat Sci 2018; 23(2): 139–149.

29. Wu D, Zhang F, Wang H, et al. Security-oriented opportunistic data forwarding in mobile social networks. Fut Gener Comput Syst 2018; 87: 803–815.

30. Zhang B, Zhang Q, Huang Z, et al. A multi-criteria detection scheme of collusive fraud organization for reputation aggregation in social networks. Fut Gener Comput Syst 2018; 79: 797–814.

31. Liu F, Zhu X, Hu Y, et al. A cloud theory-based trust computing model in social networks. Entropy 2017; 19(1): 11.

32. Chen IR, Bao F, Chang MJ, et al. Dynamic trust management for delay tolerant networks and its application to secure routing. IEEE Trans Parall Distrib Syst 2014; 25(5): 1200–1210.

33. Raj V and Balasubramanian K. Trust aware similarity-based source routing to ensure effective communication using game-theoretic approach in VANETs. J Amb Intell Human Comput 2021; 12: 1–11.

34. Kerrache CA, Lagraa N, Hussain R, et al. TACASHI: trust-aware communication architecture for social internet of vehicles. IEEE Intern Things J 2019; 6: 5870–5877.

35. Kerrache CA, Calafate CT, Cano JC, et al. Trust management for vehicular networks: an adversary-oriented overview. IEEE Access 2016; 4: 9293–9307.

36. Biswas A and Biswas B. FuzAg: fuzzy agglomerative community detection by exploring the notion of self-membership. IEEE Trans Fuzz Syst 2018; 26(5): 2568–2577.

37. Newman MEJ. Finding community structure in networks using the eigenvectors of matrices. Phys Rev E 2006; 74(3): 036104.

38. Kochemazov S. Bridging network static properties and activation dynamics. Proced Comput Sci 2017; 119: 157–165.

39. Daly E and Haahr M. Social network analysis for information flow in disconnected delay-tolerant MANETs. IEEE Trans Mob Comput 2009; 8(5): 606–621.

40. Santos EE, Korah J, Murugappan V, et al. Effectively handling new relationship formations in closeness centrality analysis of social networks using anytime anywhere methodology. In: Proceedings of the IEEE international conferences on big data and cloud computing (BDCloud), social computing and networking (SocialCom), sustainable computing and communications (SustainCom) (BDCloud-SocialCom-SustainCom), Atlanta, GA, 8–10 October 2016. New York: IEEE.

41. Hamdi S, Gancarski AL, Bouzeghoub A, et al. TISoN: trust inference in trust-oriented social networks. ACM Trans Inform Syst 2016; 34(3): 1–32.

42. http://reality.media.mit.edu/

43. Feng R, Han X, Liu Q, et al. A credible Bayesian-based trust management scheme for wireless sensor networks. Int J Distrib Sens Netw 2015; 11(11): 1–9.

44. Xia F, Liu L, Li J, et al. BEEINFO: interest-based forwarding using artificial bee colony for socially aware networking. IEEE Trans Veh Technol 2015; 64(3): 1188–1200.