Ullah, N., Kong, X., Ning, Z., Tolba, A., Alrashoud, M., & Xia, F. (2020). Emergency warning messages dissemination in vehicular social networks: A trust based scheme. *Vehicular Communications, 22.*

Which has been published in final form at:
https://doi.org/10.1016/j.vehcom.2019.100199

Emergency Warning Messages Dissemination in Vehicular Social Networks: A Trust Based Scheme

Noor Ullah[a], Xiangjie Kong[a], Zhaolong Ning[a,b,c,*], Amr Tolba[d,f],
Mubarak Alrashoud[f], Feng Xia[a,g]

[a] *School of Software, Dalian University of Technology, Dalian 116620, China*
[b] *State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210008, China*
[c] *Chongqing Key Laboratory of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[d] *Computer Science Department, Community College, King Saud University, Riyadh 11437, Saudi Arabia*
[e] *Software Engineering Department, College of Computer and Information Sciences, King Saud University, Riyadh 11437, Saudi Arabia*
[f] *Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin-El-kom 32511, Egypt*
[g] *School of Science, Engineering and Information Technology, Federation University Australia, Australia*

Abstract

To ensure users' safety on the road, a plethora of dissemination schemes for Emergency Warning Messages (EWMs) have been proposed in vehicular networks. However, the issue of false alarms triggered by malicious users still poses serious challenges, such as disruption of vehicular traffic especially on highways leading to precarious effects. This paper proposes a novel Trust based Dissemination Scheme (TDS) for EWMs in Vehicular Social Networks (VSNs) to solve the aforementioned issue. To ensure the authenticity of EWMs, we exploit the user-post credibility network for identifying true and false alarms. Moreover, we develop a reputation mechanism by calculating a trust-score for each node based on its social-utility, behavior, and contribution in the network. We utilize the hybrid architecture of VSNs by employing social-groups based dissemination in Vehicle-to-Infrastructure (V2I) mode, whereas nodes' friendship-network in Vehicle-to-Vehicle (V2V) mode.

[*] Corresponding Author: Email ID: zhaolongning@dlut.edu.cn

We analyze the proposed scheme for accuracy by extensive simulations under varying malicious nodes ratio in the network. Furthermore, we compare the efficiency of TDS with state-of-the-art dissemination schemes in VSNs for delivery ratio, transmission delay, number of transmissions, and hop-count. The experimental results validate the significant efficacy of TDS in accuracy and aforementioned network parameters.

Keywords: Emergency Warning Messages, False Alarm, Social Trust, Vehicular Social Networks, Collision Avoidance.

1. Introduction

The idea of Vehicular Ad hoc Networks (VANETs) was conceived primarily to ensure safety of users on the road. Therefore, various schemes and protocols for the dissemination of Emergency Warning Messages (EWMs) in VANETs have been proposed since its inception [1]. However, due to the short communication range of On-board Units (OBUs), most of the VANET based schemes rely on multi-hop broadcast techniques, which suffer from issues such as, broadcast storm problem, hidden node collision, network congestion, and fragile connectivity [2]. In recent past, the advent of Socially Aware Networking (SAN) [3, 4] has inspired researchers to develop new techniques for data forwarding and dissemination using social properties of the users such as, centrality, community, interests, and interactions [5], [6], [7]. Following this trend, new paradigms in vehicular communication technology have emerged such as, Vehicular Social Networks (VSNs), cloud assisted communication, and Social Internet of Vehicles (SIoVs), which offer a wide range of infotainment and safety related services [8], [9]. VSNs in particular are user driven social networks where social interactions, mobility patterns, and common interests of the users are leveraged to create different social groups and structures. Moreover, this information not only helps in developing efficient data forwarding and content dissemination but can also give an insight into anomalous behavior on the road [10, 11]. In this context, few social utility based mechanisms have also been proposed recently for dissemination of EWMs in vehicular networks to mitigate the issues faced by conventional VANET based schemes such as [12] and [13].

However, a major concern about all the EWM dissemination schemes is the veracity of the generated EWM and integrity of the originator. For example, a fake EWM generated by a malignant user may disrupt the traffic flow leading to severe consequences. Moreover, even a single occurrence of a such event may create a lack of trust in the users to believe any credible source of alert message. None of the aforementioned schemes provide any mechanism to detect such malicious node and protect users from false alarms. Therefore, to avoid such mishaps, a secure and trustworthy mechanism is of even more importance, where trust can be regarded as the degree of surety that a received message is authentic [14].

Consequently, some works have been proposed for trust establishment among nodes in VANETs such as, [15] and [16] especially for urban traffic. However, realistic initial trust values are hard to establish and maintain in these scenarios whereas sparse highway conditions offer several challenges. Similarly, very few works have been proposed for trust establishment and management in VSNs context. For instance, in [17], the authors proposed that a vehicle can be considered as a trusted social vehicle based on its degree of social activity in the network. A higher social activity degree of a node will assign it a higher trust value making it more probable to be selected as the next forwarder of a message. Similarlty, in [18], an Analytic Hierarchy Process (AHP) based trust establishment mechanism for VSNs has been proposed where social parameters such as behavior and similarity are utilized to establish trust and reputation of nodes in message forwarding. However, these schemes do not take into account the delicacy of emergency situations and only select the most trusted node to route a message from a source node to a destination. Moreover, rogue nodes can also encounter an emergency situation and may issue a true alert. Furthermore, on highways due to high mobility of the nodes, VSNs exhibit dynamic nature and rapid update of the reputation is of vital importance.

To fill the gaps, in this paper we propose a novel Trust based Dissemination Scheme (TDS) for authentic EWMs in VSNs in order to avoid false alarms. The motivation behind this work is to provide secure real-time dissemination of EWMs which is resilient to malicious attacks with realistic trust management. The contribution of this paper is manifold which is detailed below:

- We differentiate a true EWM from a fake one by analyzing the posts shared and spread by users of VSN over an extended period of time via an interaction network. Moreover, we employ a cross-check mechanism for the fake ones to avoid any rare miscalculations.

- We develop a trust estimation and management mechanism based on the reputation of nodes in VSNs by employing their social ties, behavior and contribution in the network. Furthermore, we consider VSN as a dynamic network and develop an update mechanism for the nodes' trust-score as a function of time.

- The proposed scheme calculates the probability of the next broadcaster of EWM based on higher trust-score, geographical location and speed of the nodes. In this way the redundant re-broadcasts are avoided reducing the overall network cost.
- We examine the accuracy of the proposed scheme under varying percentages of malicious nodes in the network. The results indicate high accuracy of the proposed scheme even under higher density of malicious nodes. Moreover, we present the comparison of the proposed scheme with three state-of-the-art VSNs based schemes for a variety of network performance indicators.

The rest of the paper is organized as follows: Section II gives an overview of the related work; Section III describes the network model and system overview; Section IV provides a detailed architecture and working of the TDS; In Section V we present the simulation setup and performance evaluation; Section VI concludes the paper with some future directions.

2. Related Work

Dissemination of EWMs has been extensively studied in VANETs for the last two decades via multi-hop broadcast techniques due to the short range of communication devices [1]. However, multi-hop dissemination suffers from various Quality of Service (QoS) and network issues such as, broadcast storm problem, for which various solutions have been proposed over the time [2]. Such schemes can be broadly classified into several categories depending on the technique of broadcaster selection such as, location, distance, neighbors'-table, probability, cluster, and topology based techniques. Below we categorically present some high quality recent related work to the proposed technique in this paper.

2.1. Social Network Based Forwarding Techniques

The more recent advent of VSNs has inspired researchers to explore social characteristics of the users such as, mobility pattern, interests, social interactions, and community structure for networking in vehicular environments.

For instance, in [9] the authors gave a concept of social internet of vehicles and highlighted its numerous applications in vehicular networks. In [10] an application based on trajectory data analysis to detect anomalies on the road has been proposed. Furthermore, in [19], the authors have demonstrated that socially aware and content oriented forwarding can help reduce the network cost and latency while improving delivery ratio significantly in disruptive networks. Moreover, in [20], the authors presented that social contribution of nodes in vehicular networks can be utilized to reduce the negative effects of selfish nodes in the routing process. In [21], a multi-dimensional scheme based on social features such as degree, interests, and social relationshps has been proposed to calculate a social distance metric for efficient management of time-slot allocation and forwarding of messages in SANs. Similarly, in [22] a social acquaintance metric has been derived by employing degree, contact information, and activity of the nodes for routing of messages in VSNs. However, most of these schemes provide message forwarding techniques for a predestined node in the network in contrast to spreading EWMs to a maximum number of nodes in the vehicular network.

2.2. Social Communities and Privacy

In [23], community and dynamic social features based multi-cast algorithms have been proposed achieving higher delivery ratio for mobile social networks. In [24], the authors identified that vehicles can be divided in different communities based on their social properties such as contacts and mobility patterns which can be utilized to reduce broadcast storm problem and other network issues. In [25], the authors introduced a social relationships based community partitioning mechanism for data replication in Ad-hoc Social Networks (ASNETs) in order to improve reliability and availability of the data for all users. Similarly, in [26], it has been demonstrated that network performance can be significantly improved with community-based event dissemination technique where data brokers can be clustered in a community according to their social interests and similarity and hence filter the replication. In order to identify such communities, detailed vehicular traces providing mobility information of vehicles is required. In [27], the authors used macroscopic vehicular data to identify clusters in vehicular networks for efficient routing of messages. Similarly, mobility models and datasets of large-scale urban and floating cars in VSNs have also been proposed recently [28], [29]. However, these schemes provide either synthetic traces or floating cars' data in urban scenario, which is different than a highway scenario of vehicular networks in many ways. Still these works provide incite in developing a framework for VSNs based dissemination schemes.

2.3. Social Inspired Dissemination Schemes

With the advancement of VSNs, social features based dissemination schemes have also been proposed recently [30]. For instance, in [31], a socially inspired dissemination scheme for VANETs has been proposed where next forwarder is selected based on the degree centrality of the nodes. In [32], a game-theory based approach has been presented for data dissemination in VANETs to avoid broadcast storm problem. Very recently, in [12], the authors proposed an efficient dissemination scheme for EWMs based on a social utility measure by employing social groups, friendships, and interests of the users in VSNs. However, these schemes do not offer any protection from malicious nodes which may generate a false alarm with malign intent.

In [33], an insight into measuring trust in VSNs via direct social interactions and indirect social recommendations from other vehicles has been provided. In [34], a trust and security management framework has been proposed for VANETs based on linkability information. In [35], a signalling game based approach has been adopted to mitigate selfishness and uncertain data forwarding in Moobile Social Networks (MSNs) by employing a belief system and social distance among users. In [36], the authors proposed a cloud based framework for evaluation of trust using Performance Evaluation Process Algebra (PEPA). Similarly, in [37], a three layered trust evaluation scheme for trustworthy information sharing in VSNs has been presented. In [38], a privacy preserving scheme has been proposed for secure publishing of croud-sourced data and statistics in social networks where privacy is one of the leading issues with untrusted servers. However, these schemes do not take into account the urgency of emergency warning messages and the problems related to it.

3. Network Model and System Overview

3.1. Network Model

3.1.1. Physical Network Model

We consider a hybrid VSN model where vehicles are equipped with IEEE 802.11p based On-Board Units (OBUs) along with a cellular module for communication. Moreover, Road Side Units (RSUs) are installed on various points of the highway to facilitate the communication. In hybrid model of

VSNs, vehicles can communicate in two modes: 1) Vehicle-to-Vehicle (V2V) communication between OBUs via Dedicated Short Range Communication (DSRC); 2) Vehicle-to-Infrastructure (V2I) communication between OBUs and RSUs via 3G/4G cellular network if DSRC is not reachable. Moreover, RSUs can share the gathered information with each other on a regular basis while providing a centralized monitoring system to the vehicles as well. The message transmission, network connectivity, and resource allocation are managed under standard IEEE 802.11p and cellular network protocols based on the mode of communication. In addition, each vehicle is assumed to be equipped with Global Positioning System (GPS) module that records its position on the road, speed, and time stamps in real-time. Fig. 1 illustrates the network model for the operation of TDS. The lowest layer comprises of the physical network of vehicles where communication is carried out via DSRC/WAVE or cellular transmission depending on the resource availability. The middle layer takes social network of the users into account where social properties of humans are explored to find most important and trusted nodes. The upper layer comprises of the posts-credibility network which is based on the posts shared by users over the time to identify the truth of the nature of EWM generated.

3.1.2. Social Network Model

We model a VSN as a dynamic social graph $G^t = (V, e, t)$, that evolves with time, where $V = \{v_1, v_2, \ldots, v_N\}$ is a set of vertices that represents the users driving vehicles/nodes and $E = \{(i, j) | 1 \leq i, j \leq N\}$ is a set of edges for all $i, j \in V$, which relate to the social relationships among the nodes. Moreover, we assume that nodes $i, j \in V$ may interact with each other at different intervals of time t, where these interactions are captured in a set of events $Int_i = \{i \in V \mid ev_{i_1}, ev_{i_2}, \ldots, ev_{i_M}\}$, for each node i being the observer. In addition, we assume that all nodes have specific interests, interaction circles, and affiliations, that can be organized as a set of social features $S_F = \{f_1, f_2, \ldots, f_N\}$, where $f_i = \{f_{i_1}, f_{i_2}, \ldots, f_{i_m}\}$ represents these features for each node i and $1 \leq m \leq N$. Moreover, each node has a number of friends that can be stored in a friend-list $F_{l_i} = \{x \in V \mid f_{r_1}, f_{r_2}, \ldots, f_{r_x}\}$. As in VSNs nodes can join several groups based on their interests and other social properties, we maintain a set of groups such that most similar nodes based on their social features form specific group g_i which are stored in a group register represented by the set $G_s = \{g_1, g_2, \ldots, g_L\}$. In our model the users can provide feedback on the posts of others which in a combi-

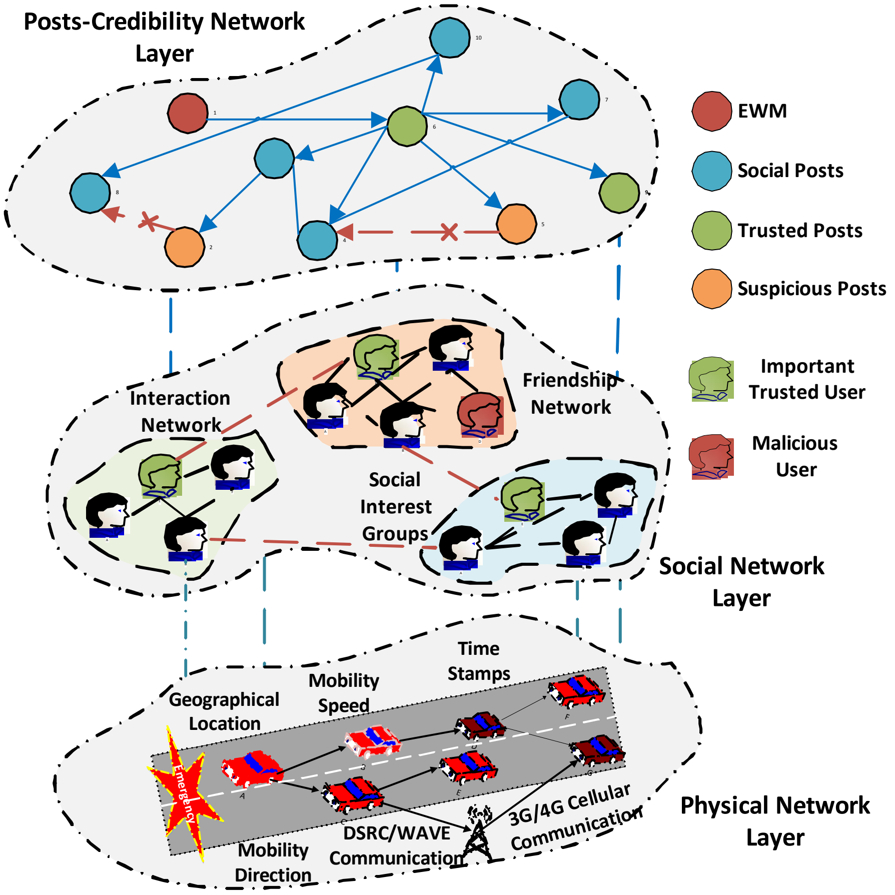


Figure 1: Illustration of the network model for the operation of TDS.

nation with other social parameters define the credibility of a node that is registered in a credibility vector $C_r = \{c_{r_1}, c_{r_2}, \ldots, c_{r_k}\}$ such that $c_k \in [0, 1]$. Similarly, the estimated trust scores of all vehicles are stored in a vector $T_S = \{T_{s_1}, T_{s_2}, \ldots, T_{s_N}\}$ such that $T_{s_i} \in [0, 1]$, for $i = 1, 2, \ldots, N$.

3.1.3. EWM and Posts

As in VSNs the OBUs and RSUs have high storage capacity, this paper does not consider the storage constraints and buffer size for messages. We assume that in normal conditions, each node i is capable of generating a set of posts $P = \{p_1, p_2, \ldots, p_n\}$, about various topics and view-points. Then each $p_i \in P$ can be labelled based on the view-points that are maintained

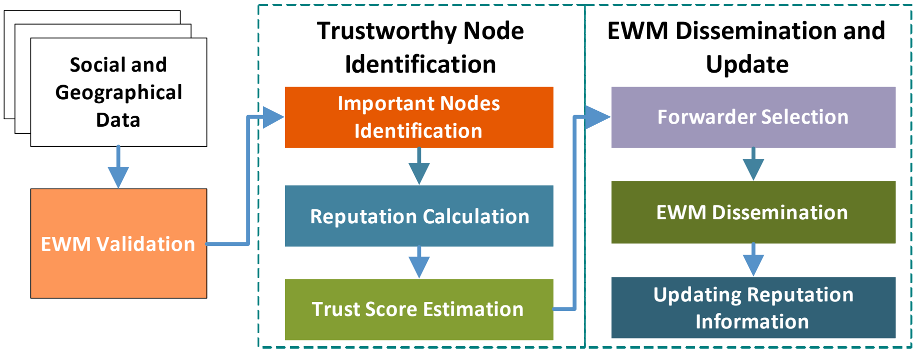

Social and Geographical Data
EWM Validation
Trustworthy Node Identification
Important Nodes Identification
Reputation Calculation
Trust Score Estimation
EWM Dissemination and Update
Forwarder Selection
EWM Dissemination
Updating Reputation Information

Figure 2: Flow diagram of TDS.

in a vector space $L = \{l_1, l_2, \ldots, l_k\}$ such that $l_i \in [0, 1]$ for $1 \leq i \leq k$ represents the weight of each of the view-points. Similar to [39], we assume that each post has the following attributes: 1) a unique ID of the post; 2) the originator's ID, Ori_p; 3) distantions ID, Des_p; 4) The Time-To-Live TTL of the post, ttl_p. On the other hand, we treat EWM differently than normal posts as it contains only one viewpoint i.e., warning about an emergency. Each EWM contains the following attributes: 1) Source Vehicle's ID, ID_{Src}; 2) Origination time of the EWM t_{ori}; 3) Location of the source vehicle Loc_{src}; 4) Location of the emergency point Loc_{EmP}; 5) Type of emergency, T_{Em}; 6) the Time-to-Live, ttl_{EWM} after which EWM will be discarded; and 7) the broadcaster's ID, ID_{Br}.

3.2. System Overview

The proposed scheme considers the severance of fake EWMs in a highway scenario, where vehicles may face rear-end collision leading to vehicles pile up on the road. Such a mishap can have a severe disastrous outcome. On the other hand, a timely generated alert about any mishap on the road reduces the chances of severe calamities by a significant amount. Therefore, we devise a mechanism to avoid such false alarms along with efficient dissemination of genuine EWMs in VSNs. Fig. 2 provides a flow diagram for the proposed mechanism. Below is a brief detail of each step and component of TDS.

3.2.1. EWM Validation

The first and foremost step of the proposed scheme is to verify the authenticity of the EWM issued by a vehicle. We consider this problem as the propagation of fake news in a social network and hence deal with it using a user-post interaction and credibility network. This operation is carried out by the *EWM validation* component of TDS based application. Therefore, each node stores its social and geographical data in specified registers of their OBUs, which is passed on to another vehicle upon each interaction in an opportunistic manner. This data include social media posts, location information, opinions of the nodes on different topics, which are used to calculate the credibility of users and the authenticity of the posts. If a EWM is identified to be genuine, based on credibility of the source vehicle, then it is forwarded to the most suitable nodes that can spread it as fast as possible. On the other hand, if EWM is verified to be of fake nature, then it is still validated by the receivers for authenticity.

3.2.2. Important Nodes Identification

Once a true alert is validated, then the proposed scheme calculates the social importance of nodes in the network using *important nodes identification unit*. Because a highly important node is usually the most connected and followed by others, it is more capable to spread the EWM to a higher number of nodes significantly. For this purpose, TDS calculates the social centrality of each node in the network, its similarity with other nodes, and its interaction network based on various social features such as, interests, social contacts, and activity in the network. By using the aforementioned metrics, we derive a social utility function that determines how useful a node i can be to other nodes in disseminating messages. Due to dynamic nature of VSNs, these social metrics change as the time progresses, therefore we devise a regular update mechanism for these metrics. In this way most recent information is utilized for dissemination purpose

3.2.3. Reputation and Trust Calculation of Nodes

To deal with malicious nodes, we build a reputation and trust establishment mechanism for nodes in the VSN via a *reputation and trust estimation unit*. We consider several factors such as a user's behavior, its social contribution in the network, and its social activity to calculate its credibility in the views of other nodes. Then by voting and feedback of other users, a reputation along with its credibility is built over time. This is done in a recursive manner where a node's reputation score is called in the voting function. The reputation of the node essentially changes with time, therefore we update the reputation information of nodes in a given interval of time. A node's reputation and its social utility are employed in conjunction to estimate a trust score for each node which helps eventually in avoiding fake EWMs. The updated information is shared with other nodes upon each interaction.

3.2.4. Broadcaster Selection and Dissemination

In order to efficiently disseminate a genuine EWM in the network, we benefit from the hybrid model of VSNs. Therefore, we employ both V2V and V2I mode of communication based on the resource availability. Moreover, we utilize social groups and friendships of the users to disseminate EWM in respective groups and friendship networks for rapid delivery. For this purpose, the most trusted nodes are given a higher priority in broadcaster selection whereas within groups higher social utility nodes are selected to broadcast it in their respective groups.

4. DETAILED DESCRIPTION OF TDS ARCHITECTURE

In this section we explain the architecture of a TDS based application and give a detailed description of the construction and operation of its various units. Moreover, we explain the algorithm developed for the dissemination of EWMs in TDS under V2V and V2I strategies, based on the resource availability. Fig. 3 demonstrates a detailed block diagram of the architecture of TDS based application unit.

4.1. Message Handling

The proposed algorithm first collects the social and location data of the vehicles in the network. To detect the authenticity of the EWM, we consider a heterogeneous user-post interaction network. We consider that a false alarm can be treated as a fake news in the social networks, therefore, we deal with this problem as of a fake news detection. The data collected is used to identify the credibility of nodes based on trust score that is maintained in vector space T_S. Vehicles with low credibility are more likely to raise a false alarm than the higher ones. By employing the Non-negative Matrix Factorization (NMF) method, the document-word matrix can be used to find a non-negative matrix $Y \in R^{n \times d}$ representing the posts. Similarly, the vehicles' adjacency matrix $A \in \{0,1\}^{N \times N}$ can be used to obtain a non-negative matrix $X \in R^{N \times d}$ representing the users of the posts [40]. The posts shared by the users are partially labelled which are maintained in a vector space $L_p = (l_{p_1}, l_{p_2}, \ldots, l_{p_K})$ where $l_{p_i} \in [0,1]$. In order to identify if any

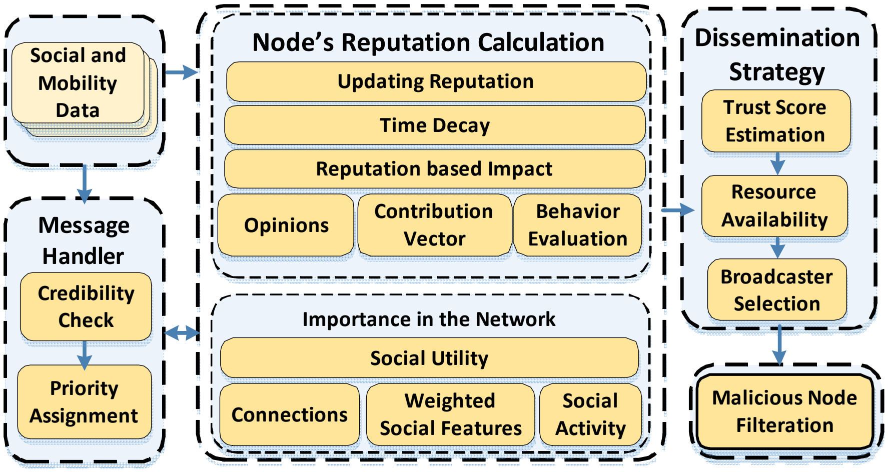


Figure 3: Block diagram of detailed architecture of TDS application unit.

node i has engaged in the spreading process of a specific post, we maintain a vehicle-post engaging matrix $E \in \{0, 1\}$ of the order $N \times N$ as given in (1):

$$E = \begin{bmatrix} e_{11} & e_{12} & \cdots & e_{1N} \\ e_{21} & e_{22} & \cdots & e_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ e_{N1} & e_{N2} & \cdots & e_{NN} \end{bmatrix}, \tag{1}$$

where $e_{ij} = 1$ if i_v engaged in spreading e_j and 0 otherwise. Then we can separate a true EWM from a false one similar to [41] as:

$$P_T = \min \sum_{i=1}^{N} \sum_{j=1}^{m} e_{ij} \cdot T_{s_i} \left(1 - \frac{1 + L_{p(j)}}{2}\right) \|Y_i - X_i\|_2^2, \tag{2}$$

$$P_F = \sum_{i=1}^{N} \sum_{j=1}^{m} e_{ij}(1 - T_{s_i}) \left(1 - \frac{1 + L_{p(j)}}{2}\right) \|Y_i - X_i\|_2^2. \tag{3}$$

When it is established that the EWM generated is not a false alarm then it is given a special priority status in the medium access and communication network. However, as the authenticity of EWM is determined based on the credibility of nodes along with other aforementioned factors, a false alarm cannot be completely neglected as well because a low-credibility node can also suffice a very real emergency at any time. Therefore, to consider such a scenario, a EWM flagged as false alarm is still broadcast to the nearest vehicles in range. However, only the receiving vehicles that are nearest to the indicated anomaly location keep a suspicious EWM for further validation while others discard it. Being in line of sight of the anomaly location and closer to source vehicle, which can be calculated similar to [12], the receivers decide whether the emergency is real or not by observing the situation. If the generated EWM is found to be authentic, then the farthest vehicle from the anomaly location is selected as the broadcaster which further broadcasts it according to TDS protocol. On the contrary if EWM is still deemed as a false alarm then it is discarded immediately and the source vehicle is blacklisted. All other vehicles are informed about the suspicious vehicle and its false alarm.

4.2. Node's Importance Calculation

For reliable broadcast of authentic EWM, the most suitable and trustworthy nodes in the network must be identified. Therefore we exploit social properties of the nodes in the network such as, similarity, community, interactions, and centrality to select the most important nodes in the network. Due to high mobility of the vehicles, VSN can be considered as a dynamic network where the properties of the nodes may change with time. Moreover, dissemination of EWMs in the VSN is a spreading phenomenon which has the tendency of percolation. We consider a scenario where a source vehicle $i \in V$, undergoes a change in percolated state from $s_i^t = 0$ to $s_i^t \leq 1$ upon initiation of the EWM. As an example, if we divide nodes into states s_1 and s_2 where s_1 represents that the node is not informed yet and s_2 means that node has been informed. This change of state in terms of its activity over time also imparts a change of state in the target vehicles from states $s_i^t \in [0, 1]$ depending on their previous states. Therefore, we employ percolation centrality, C_p [42] to calculate the importance of nodes in VSN for dissemination of EWMs for any time t. For any node $i \in V$, C_p is the proportion of percolated paths that go through it, at any given time interval t which is given as:

$$C^t_{p(j)} = \sum_{i \neq j \neq k}^{N} \frac{\mathscr{G}_{i,j}(k)}{\mathscr{G}_{i,j}} \times \omega^t_{i,j,k} \ , \tag{4}$$

where $\mathscr{G}_{i,j}(k)$ is the number of geodesic paths between nodes i and j that pass through k, whereas $\mathscr{G}_{i,j}$ is the total number of geodesic paths between nodes

i and j, and $\omega^t_{i,j,k}$ is a weighting factor of the percolated paths of source and receiving nodes which is given as:

$$\omega^t_{i,j,k} = \frac{R(s^t_i - s^t_k)}{\sum^N_{i \neq j \neq k} R(s^t_i - s^t_k)} \ , \tag{5}$$

where $R(s^t_i - s^t_k)$ is a Ramp function $R(s) = s$ for a positive value of s and 0 otherwise. Based on this criteria, the proposed algorithm calculates the social position $S^t_{p_{(i)}} \in [0, 1]$ of each node i in the network by exploring the importance of node i and its neighboring nodes in the network, which is utilized to weight the opinion of node i. This information is shared with other nodes upon every interaction. However, as the time progresses, this information changes due to topological changes and the dynamic nature of VSNs. Therefore, similar to [14], we calculate the social position of each node in VSN by employing $C^t_{p(i)}$ instead of simple degree value, at any given time t as:

$$S^{t+\Delta t}_{p(i)} = \begin{cases} \frac{C^t_{P(i)}}{\max\limits_{m \in V} C^t_{P(m)}} & at\ t = 1 \\ S^t_{p(i)} + \sigma^2 \cdot S^{t-\Delta t}_{P(i)} & otherwise \end{cases} \ , \tag{6}$$

where the denominator represents the maximum percolation centrality of a node in the network and σ is the priority constant whose exponent determines the speed of variance of node i's influence at time t for an interval Δt which can be calculated similar to [43].

According to *homophily theory*, nodes with similar interests are more likely to befriend with each other [39]. This phenomenon leads to a faster dissemination of messages among friends. Similarly, vehicles can be categorized into various communities/groups based on their interactions. Therefore, we categorize nodes into social similarity based groups. To calculate similarity of the nodes we use *Jackard Similarity Coefficient* based on their social features. However it is understood that some features may influence the relationship more strongly than others, therefore, we calculate weights for each feature $x \in f_i$ of node i similar to [44] as:

$$w_i(x) = \frac{f_i(x)}{\sum^N_{j=1} f_j(x)} \bigg/ \sum^M_{k=1} \frac{f_i(k)}{\sum^N_{j=1} f_j(x)} \ . \tag{7}$$

Then substituting each value of x with the weighted value we get a set of weighted feature values as:

$$f^w_i = w_i(x) \times f_i(x)|^N_{x=1} \ . \tag{8}$$

The similarity value between nodes i and j for any feature x can then be found using (9) whereas overall similarity for all the features is given in (10).

$$sim^{x}_{(i,j)} = \frac{|f^{w}_{i} \cap f^{w}_{j}|}{|f_i \cup f_j|} \ , \tag{9}$$

$$sim^{f_i \cup f_j}_{(i,j)} = \frac{1}{m} \sum_{x \in (f_i \cup f_j)} sim^{x}_{(i,j)} \ . \tag{10}$$

The overall similarity between any two nodes for all the features at any given time t can then be calculated as follows:

$$sim^{t+\Delta t}_{(i,j)} = \begin{cases} sim^{f_i \cup f_j}_{(i,j)} & at\ t = 1 \\ sim^{t}_{(i,j)} + \sigma^2 \cdot sim^{t-\Delta t}_{(i,j)} & otherwise \end{cases} \ , \tag{11}$$

where the meaning of σ remains the same as in (6) and depends on the social activity of the nodes. Each node maintains a table of similarity values with its connected nodes.

In any social network, the interaction between users is of significant importance and reveals important information about users' social relationships, behavior, and their classification into various communities. This argument is further validated by extracting data from *hycoups dataset* [45]. In this dataset the social contacts' data of 72 users over a period of time from their social profiles is obtained that contains their social interactions information with each other. After extracting the data we observed that users were classified into five distinct communities based on the number of interactions and contacts they had in common which is given in Fig. 4. We take this measure into account to derive social ties among nodes as follows: We consider a scenario where a node $i \in V$, interacts with a number of nodes $V_{int} \subset V = \{v_1, v_2, \ldots, v_L\}$ and the number of interactions are recorded in the vector Int_i. By more frequent interactions, each node $i \in V$ establishes a community. Then the total number of interactions of node i with all the other nodes in its community can be found as:

$$N_{int(i)} = \sum_{j=1}^{N} \sum_{k=1}^{L} a_k(i,j) \ , \tag{12}$$

where $a_k(i,j) = 1$ if nodes i and j have contacted each other and 0 otherwise. As similarity between nodes i and j is a strong indicator of their tie-strength

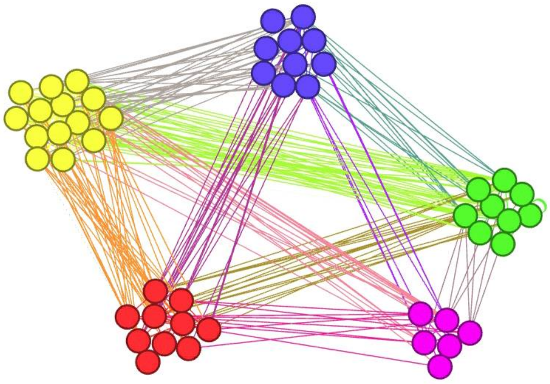


Figure 4: An example of community formation based on interaction of nodes.

[39], their interactions network can also be of great importance as well in providing more accurate incite on tie-strength of two nodes [20]. Therefore, we formulate a Tie-Strength metric for nodes i and j by employing their $sim^t_{(i,j)}$ value calculated in (11) and their interactions network as:

$$TS_{(i,j)} = \gamma \cdot \left(\frac{2 \times N_{int(i,j)}}{N_{int(i)} + N_{int(j)}} \right) + (1-\gamma) \cdot sim^t_{(i,j)} \ , \tag{13}$$

where $N_{int(i,j)}$ indicates the number of times node i interacts with node j, and $\gamma \in [0,1]$ is a normalization constant whose value can be adjusted to incline the dependency of $TS_{(i,j)}$ toward similarity or interactions network of these nodes. Since interaction between nodes i and j is a bidirectional phenomenon, therefore we use a multiplicative factor of 2 in (13). From (6) and (13), we can then calculate the social utility value of a node i to any node $j \in V$ in the network as:

$$U^t_{s(i)} = \alpha \cdot S^t_{p(i)} + (1-\alpha) \cdot \sum_{j \in V} T_{s(i,j)} \ , \tag{14}$$

where $\alpha \in [0,1]$ is a normalization constant that can shift the tendency of utility to either $S_{p(i)}$ or $TS_{(i,j)}$. A higher social utility value of a node gives it higher priority to be selected as next forwarder.

4.3. Reputation Calculation

In order to calculate the reputation of nodes, we consider two important parameters i.e., social contribution and evaluation of nodes by their socially connected nodes. As we have seen that nodes can be categorized into various groups based on their interactions, so we use this interaction information to quantify the social contribution. Upon every interaction, nodes i and j may share some messages based on which we can formulate the contribution of a node i toward node j as:

$$C_{i(j)} = \sum_{j=1}^{L} \frac{N_{pr_{i(j)}}}{N_{pr_{i(j)}} + N_{ps_{i(j)}}} \ , \tag{15}$$

where $N_{pr_{i(j)}}$ indicates the number of packets i has received from node j and $N_{ps_{i(j)}}$ represents the number of packets sent by node i to node j. However, it is of utmost importance to find how much node i facilitates other nodes in its community by forwarding their messages to the destined nodes. For instance, if node i has connections with nodes j and k whereas the latter nodes are not connected directly. If node j wants to send a message to k and asks i to forward it, then node i facilitates the communication between nodes j and k. Therefore this facilitation is of utmost importance in calculation of node i's contribution which can be calculated as:

$$X_{i(j,k)} = \frac{\sum_{j \neq k \in V}^{n} N_{ps_{i(j,k)}}}{N_{p_i} + \sum_{j=1}^{n-1} N_{ps_{j(k)}}} \ , \tag{16}$$

where $N_{ps_{i(j,k)}}$ represents the number of packets i forwards from node j to node k and N_{p_i} is total number of posts node i has generated while $N_{ps_{j(k)}}$ is the number of packets sent by node j to k. Then we can obtain the social contribution of node i as:

$$S_{c(i)} = \mu(C_i) + (1 - \mu)(X_{i(j,k)}) \ , \tag{17}$$

where $\mu \in [0, 1]$ is a weight factor to control the dependence of S_{c_i} on node i's contribution and facilitation which can be calculated using social relation between nodes i,j and k as:

$$\mu = \frac{\sum_{j \neq k} \mathscr{G}_{j,k}(i)}{N_{int_{(i,j)}} + N_{int_{(i,k)}}} \ . \tag{18}$$

In online social networks a post's credibility is evaluated by the help of likes and dislikes it receives from other users. Usually a higher number of likes on a post defines its acceptability whereas a higher number of dislikes determines its rejection. We use a similar concept to evaluate the content shared by users in the VSN over a time interval t. A higher number of positive reviews over a number of posts p_n gets a positive rating for users while negative reviews earn them negative rating. Therefore, we formulate the behavior of node i based on such reviews as:

$$B_i = \frac{\sum_{j \in V} \sum_{k=1}^{n} |PR_{k(j)} - NR_{k(j)}|}{|P_i|} \ , \tag{19}$$

where $PR_{k(j)}$ means positive review for k_{th} post of i by node j and $NR_{k(j)}$ means negative reviews. Using (17) and (19), we can calculate the evaluative credibility of node i by other nodes $j \in V$ at any instant of time t as:

$$C^{t+\Delta t}_{r_{i(j)}} = \begin{cases} \beta \cdot S_c + (1-\beta) \cdot B_i & at\ t = 1 \\ C^{t}_{r_{i(j)}} + \sigma^2 \cdot C^{t-\Delta t}_{r_{i(j)}} & otherwise \end{cases} \ , \tag{20}$$

where β is a normalization constant that decides dependence of credibility value on S_c and B_i. The obtained $C^{t}_{r_{i(j)}}$ is stored in vector C_r defined in Section III. Then we can calculate reputation of each node for single interaction based on the views of other nodes per instance of interaction in a recursive manner as:

$$R^{int}_{i,j} = \sum_{j \in V} C^{t}_{r_{i(j)}} \times F^{int}_{i,j} \ , \tag{21}$$

where $F^{int}_{i,j}$ is the feedback it receives upon each interaction from other nodes and is called upon recursively in the reputation function. We calculate a self-evaluation value $E_{(i)}$ for each node to ensure that a group of malicious nodes do not alter the reputation of a single node. Therefore, we consider the views of the friends of node i about node j based on which it evaluates node j, which is represented by $x_{ij} \in [0,1]$. Each view of a friend of node i plays a role in evaluation of node j's status as a trusted or untrusted node, therefore, similar to [46] we derive a matrix AX such that:

$$AX = \begin{bmatrix} a_1^1 \cdot x_{11} & a_2^1 \cdot x_{12} & \dots & a_1^M \cdot x_{1K} \\ a_1^2 \cdot x_{21} & a_2^2 \cdot x_{22} & \dots & a_2^M \cdot x_{2K} \\ \vdots & \vdots & \ddots & \vdots \\ a_1^M \cdot x_{M1} & a_2^M \cdot x_{M2} & \dots & a_M^M \cdot x_{MK} \end{bmatrix} \ , \tag{22}$$

where $a_i^j = 1$ if i considers j credible and 0 otherwise. To ensure that

$a_i^j \cdot x_{i,j} \in [0,1]$, we normalize the matrix as:

$$ax_{ij} = \begin{cases} \frac{a_i^j \cdot x_{ij}}{\sum_n a_n^j \cdot x_{jn}} & if\ a_i^j \cdot x_{ij} \neq 0 \\ 0 & otherwise \end{cases} \quad .$$

Then the self-evaluation can be aggregated as:

$$E_{(i)} = (AX^T)^K \cdot ax_i \ . \tag{23}$$

As the feedback of highly important nodes is given a higher priority. Therefore we formulate the feedback function as:

$$F_{i,j}^{int} = U_{s(i)}^t \times E_{(i)} + (1 - U_{s(i)}^t) \times R_{i,j}^{int} \ . \tag{24}$$

4.4. Trust Score Estimation

We calculate the trust score for each node based on its reputation which is then used to select a node for broadcasting the EWM in the VSN. Due to the highly dynamic nature of VSN, the reputation of nodes cannot remain static and is dependent on time and diameter of its social circle. Therefore, to update the reputation of nodes we consider the decay of reputation value based on the velocity of the events e_i and e_j. For instance if event e_i is moving at velocity vel_{e_i} and event e_i with vel_{e_j}, then the acceleration r of these events can be calculated as:

$$r = \frac{vel_{e_i} - vel_{e_j}}{\Delta t} \ . \tag{25}$$

Keeping in view the acceleration of events, we can calculate an impact function to increase or decrease the feedback of nodes with the passage of time similar to [14] as:

$$R_{imp(i)} = |r| \times {F_{i,j}^{int}}^{\frac{-3r}{|r|}} + (1 - |r|) \times F_{i,j}^{int} \ . \tag{26}$$

Similarly, as the time progresses the reputation of nodes may increase or decrease based on their activity in the network. Therefore, we use exponential decay function along with impact function of reputation to update its value at a given instance of time using (27) as:

$$R_{i,j}^t = e^{-\tau} \cdot R_{i,j}^{t-\Delta t} + (1 - \tau) \cdot R_{imp(i)} \ , \tag{27}$$

where the value of τ determines the rate of decay of the reputation value of node i by node j. Then the trust score for node i in the whole network can be given as:

$$T^t_{s(i)} = \frac{1}{N-1} \sum_{j \in V} R^t_{i,j} \ . \tag{28}$$

The trust score is propagated among the nodes over the time per interaction. The nodes with higher trust scores are most probably going to improve their reputation. On the other hand, malicious nodes will not gain higher reputation because of their behavior while their $R^t_{i,j}$ will decay as the time goes on, earning them least T_s value and eventually will be discarded from the dissemination network.

4.5. Dissemination Strategy for EWMs

For efficient dissemination of authentic EWMs, we developed an algorithm which is illustrated in Fig. 5. The pseudocode is presented in Algorithm 1 and is explained as follows: In case of an emergency, a vehicle generates a EWM and broadcasts it to other vehicles and RSUs in its vicinity. The generated EWM is checked for authenticity using (2) and (3). If it is validated as a true warning then the dissemination process is started immediately. In case if it turns out to be of suspicious nature, then the receiving nodes and RSUs cross check it via nearest vehicles to the source vehicle. If they validate the EWM then the dissemination process is initiated. Similar to [12], we consider the infrastructure support vital for our dissemination strategy. In case if there is an RSU in the range then infrastructure based dissemination is employed because of the higher resource availability and efficacy. Therefore, RSU determines the priority for broadcaster selection based on the speed, location, mobility direction, trust-score and the social utility of the vehicle. As demonstrated in [12] and [47] that dissemination via social groups achieve higher efficiency, we employ similar strategy in V2I mode. However, we consider groups based on similarity of nodes over social features calculated in (10). Therefore, nodes i,j with higher similarity are considered as members of a group g_i as compared to node k with less similarity and is given for realistic approximation as:

$$\forall i, j, k \in V; \ g_i = \{i, j\}, \ if \ sim^F_{(i,j)} > sim^F_{(i,k)} \ .$$

Each group is managed by a group administrator that determines the acceptance or rejection of new members into the group and removal of disruptive members. The criteria for decision on admission request is also based on the cumulative similarity of a group such that:

$$Adimisson\ Request = \begin{cases} Reject, & sim_{(i,g_i)}^{f_i \cup f_{g_i}} < g_{ith} \\ Accept, & otherwise \end{cases},$$

where $g_{i_{th}}$ is a threshold value for each group. Instead of selecting one broadcaster, TDS selects highest T_s value nodes to forward the EWM to highest $U^t_{s(i)}$ value nodes in each group whereas rest of the functionalities of groups are similar to [12]. As speed of the vehicles have a direct impact on the propagation of the messages, therefore a vehicle with highest mobility is selected

Algorithm 1 Pseudocode for TDS

```
 1: Initialization: $\forall i \in V \rightarrow U^t_{s(i)},\ T^t_{s_i}$, EWM generate
 2: if $EWM = P_F$ then
 3:    validate $\rightarrow Neighbors(V_{received}, \min Dis_{Emp})$
 4:    if True then
 5:       Terminate
 6:       Blacklist$\rightarrow V_{src}$
 7:    end if
 8: else if $EWM = P_T$ then
 9:    for $t \leq ttl_{EWM}$ do
10:       if RSU is in range then
11:          Initiate $\rightarrow$ V2I Mode
12:          $V_{received} \subset V, \rightarrow$ Select $\max T^t_{s_i}$
13:          $\forall g_{joined} \in G \rightarrow$ forward $\max(U^t_{s(i)}, V_{speed})$
14:          broadcast $\rightarrow g_i|_{i=1}^{L} \in G,\ f_{r_x} \in F_{l_i}$
15:          Jump to 12
16:       else
17:          Initiate $\rightarrow$ V2V Mode
18:          $V_{received_i} \subset V \rightarrow$ broadcast to $F_{l_i}$
19:          $f_{r_x} \in F_{l_i} \rightarrow$ Select $\max(T^t_{s_i},\ U^t_{s(i)}, V_{speed})$
20:          Scan RSU $\rightarrow$ if in range, jump to 12
21:          else broadcast to $(F_{l_x},\ \max S^t_{p(i)}|_{i \in V})$
22:          jump to 18
23:       end if
24:    end for
25: end if
```

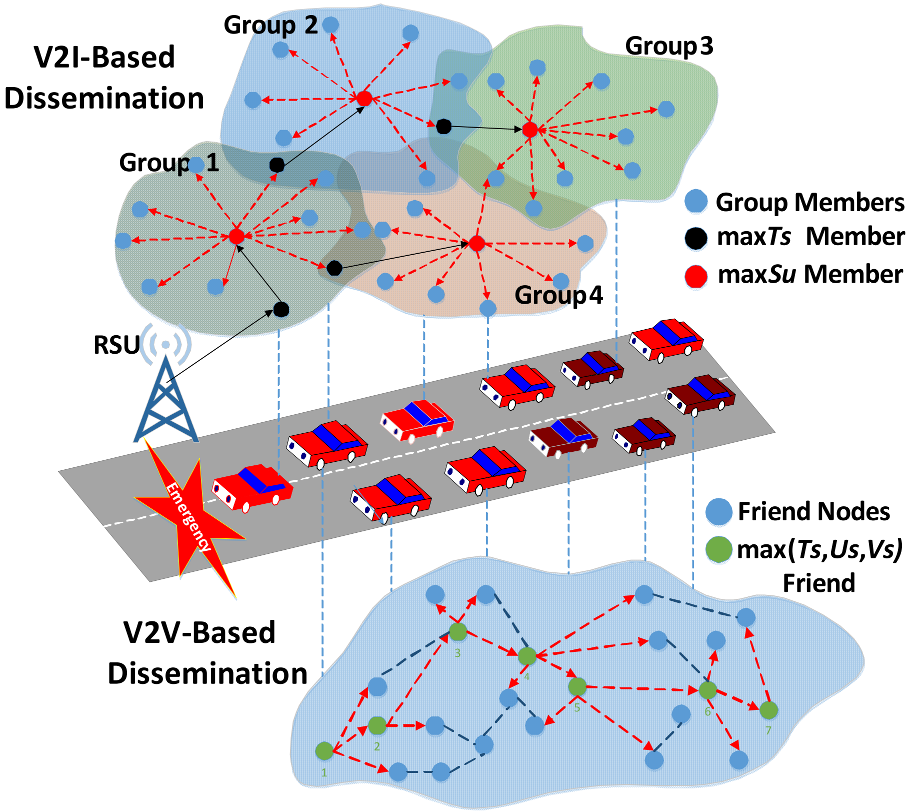


Figure 5: An illustration of TDS based EWM dissemination strategy.

in case of two nodes having same $U^t_{s(i)}$ value. Among the received nodes in each group, the highest T_s value node with the farthest location from the source node is selected to broadcast the EWM to the highest $U^t_{s(i)}$ value in each group it has joined, which again broadcast the EWM in the respective groups. In case if there is no RSU in range, then V2V mode is activated. As it is evident from Fig. 4 that higher social interaction results in social communities, therefore we can infer a fast dissemination probability within such communities. We consider friendship based communities where friendships of nodes are maintained over time based on historical data of interactions, and similarity in F_{l_i} where friendship identification technique is similar to [12]. However we employ similarity in conjunction with contacts to identify nodes as friends. Therefore upon receiving a EWM, nodes broadcast it to their friends, $f_{r_1}, f_{r_2}, \dots, f_{r_{N-1}} \in F_{l_i}$. In the next iteration, the highest $U^t_{s(i)}$ valued friend is selected as broadcaster to its friends. Priority is given to a node that is farther than the source node's location. Upon reception the received nodes search for RSU and if there is an RSU then V2I mode is enabled. If there is no RSU then the receiving nodes broadcast the EWM to all the nodes in their range and the same procedure is repeated until the ttl_{EWM} is reached to its limit.

5. EXPERIMENTS AND PERFORMANCE EVALUATION

5.1. Experimental Setup

In order to evaluate the performance of TDS, we generated synthetic vehicular traces for a 3 *km* highway scenario with 4-lanes in each direction using VANETMobiSim, which is a very powerful and well known vehicular mobility generation simulator. The reason for using synthetic mobility traces is the lack of social data availability for vehicular networks especially in highway scenario. Although some realistic vehicular mobility traces are available, they do not offer the flexibility to incorporate social features required for VSN environment. In our experiments we employ Random Waypoint Model for the mobility of vehicles, with a speed ranging from 60 km/h to 120 km/h. Furthermore, to evaluate scalability of the proposed scheme, we varied the density of vehicles between 10 vehicles/km and 70 vehicles/km. Each node employs IEEE 802.11p standard for V2V communication via WAVE/DSRC, having a communication range of 80 meters. For V2I communication we installed 10 RSUs, each having a communication range of 300 meters at random points. The packets are generated and transferred at a rate of 1Mb/s. A list of the details of network parameters is given in Table 1. We assume that no node behaves selfishly and all nodes are fully cooperative for the purpose of simplicity. In order to impart social features to the nodes such as interests, interactions, friendships, and groups, we simulated the generated traces in ONE (Opportunistic Network Environment) simulator, which is designed in Java for opportunistic communication and is very flexible to incorporate such social features. Therefore, we converted the traces into *wkt* format which is compatible with ONE.

To analyze the social features and properties of the nodes, we setup the simulation such that all nodes are capable of generating and receiving social posts based on their interests, interactions, and group activity. The number of posts is determined by the activity of the nodes that evolve over time.

Table 1: Simulation Parameters

Parameter	**Value**
Network Simulator	ONE
Trip generation	Random waypoint model
Simulation duration	2000 s
Vehicular density	10-70 vehicles/km
Road length	3000 m
Speed of vehicles	60-120 km/h
CBR	0.2 s
Transmission range of nodes	80 m
Transmission range of RSUs	300 m
MAC protocol for V2I	IEEE802.11p
Malicious nodes	10-70%

Similarly, all nodes are capable to evaluate others and provide feedback on the posts shared by either liking or disliking them. For this purpose, we assigned each node an initial behavior probability $p_b \in [0, 1]$, randomly. For instance, a node i with $p_b = 0.5$, may generate a true or false alert with an equal chance. Similarly, it may provide a negative or positive feedback on the posts of other nodes with equal probability. Therefore, at $p_b = 0.5$, its behavior is unpredictable and we consider 0.5 as the seed value for all vehicles upon initiation. On the other hand, vehicles with $0 < p_b < 0.5$ have a higher tendency to create false alerts and negative feedbacks on genuine posts of other nodes, therefore such nodes are considered relatively malicious. However, a node with $p_b = 0$ will always create a false alert and will always provide negative feedback on the genuinely true posts of other nodes and therefore it is considered a purely malicious node. As the time passes, the behavior probability of nodes may change based on their activity which is recorded and processed accordingly. However, to evaluate the performance of TDS, a percentage of malicious nodes ranging from 10% to 70% are inserted in the network. However, we assume that all nodes give a true feedback based on their assessment of the nature of post. Therefore, we set a warm up time of 24 hours to build reputations and trust of vehicles before analyzing them for our desired EWM dissemination strategy.

5.2. Performance Evaluation

To evaluate the performance of TDS, we conducted extensive experiments by varying density, distance, TTL, and speed of vehicles for a variety of network parameters that are listed below:

- *Average delivery ratio* is the mean value of the ratio of total number of receiving nodes to the total number of nodes in a given network. Ideally its value should be 100% but due to practical limitations it may not reach to maximum value in most cases.

- *Average transmission delay* is the time taken by the EWM to propagate in the network completely and cover the whole scenario. Due to sensitivity of the situation transmission delay should be as less as possible.

- *Total number of transmissions* is the number of generated messages that are transmitted in the whole network with multiple copies and re-broadcasts as well. To avoid broadcast storm problem, bandwidth wastage, network congestion, and cost, the total number of transmitted messages should be as minimum as possible.

- *Time-to-Live (TTL)* is the duration of time for which a EWM will propagate in the network to avoid unlimited circulation.

- *Hop-count* is the total number of selected broadcasters that spread the message to the far end of the network covering the whole length of the road and vehicles.

In order to analyze the performance of TDS under the presence of malicious nodes in the network, first we conducted experiments by inserting malicious nodes in the network in a range of percentages. Then we observed its performance for the aforementioned parameters under varying speed, density, TTL, and distance. Moreover, we also measured the cumulative social trust that built up over the time of simulation for different values of α and β. Secondly, to compare the performance of TDS, we set a criteria to select protocols that use social metrics for dissemination of messages in a VSN environment. Therefore, we selected the following state-of-the-art social metrics based protocols for dissemination in VSNs:

- Social Utility based Dissemination Scheme (SUDS) [12] is a EWM dissemination scheme that employs social properties such as centrality, friendships, and groups of users for V2V and V2I communication modes in VSNs

- SCARF [17] is a robust dissemination protocol for VSNs that calculates probability using social properties and location, for next forwarder selection and collision avoidance in vehicular networks.

- Social-aware Bootstrap Trust Evaluation (SBTE) [18] is a reputation based scheme for dissemination of messages in vehicular networks where the reputation is calculated based on some social parameters such as experience in driving and behavior of users.

We ran simulations 10 times for each experiment and the results presented below represent the average of those simulation data.

5.2.1. Accuracy of TDS

To obtain the rate of cumulative social utility gain by the nodes with the passage of time for different values of σ, we have given the results in Fig. 6 for a duration of 500 seconds for comprehensive understanding. A higher value of σ means a lower weight is given to the social metrics at time $t - \Delta t$ as compared to the current values at time t. We varied the value of σ from 0.1 to 0.9 for an extended duration of time. From the results it is evident that the cumulative social utility of nodes increases for all values of σ as the time progresses due to the positive reviews and behavior of highly credible nodes. However, the rate of improvement is much higher when the value of σ is chosen smaller. For instance, at $\sigma = 0.1$, the rate of improvement in CSU is 49.8% higher than that of at $\sigma = 0.9$. These findings indicate the recency of social metrics of nodes is of utmost importance in calculation of the social utility of the nodes.

To observe the effect of α and β on the values of $U^t_{s(i)}$ and $C^t_{i(j)}$ of a node i respectively, with the passage of time, Fig. 7 represents their values for a duration of 1000 seconds where maximal values are achieved. It can be observed that at lower values of α and β i.e., 0.3 the social utility and credibility of an individual node vary at a slower rate whereas at a higher value such as 0.7, the rate of change is much higher. For instance the rate of improvement of $U^t_{s(i)}$ at α=0.7 is 25% and 35% higher than that of at α=0.5 and α=0.7 respectively, while its value improves 14.4% faster at α=0.5 as compared to at

α=0.3. Similarly, the rate of change in $C^{t}_{i(j)}$ of a node is 33% and 7% higher at β=0.7 than that of at β=0.3 and β=0.5. From these observations we can conclude that in a nodes social utility the role of its Tie-Strength is of higher importance than its interaction network. A higher weight allotted to $TS_{i,j}$ will result in higher rate of social utility improvement and update. Similarly, in credibility of the node, its social behavior plays a bigger role than its total social contribution. Therefore, users should pay higher attention to their

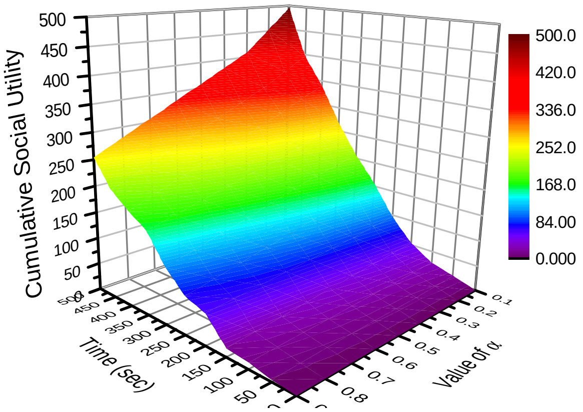


Figure 6: Effect of different values of σ on cumulative $S_{u(i)}$ against time.

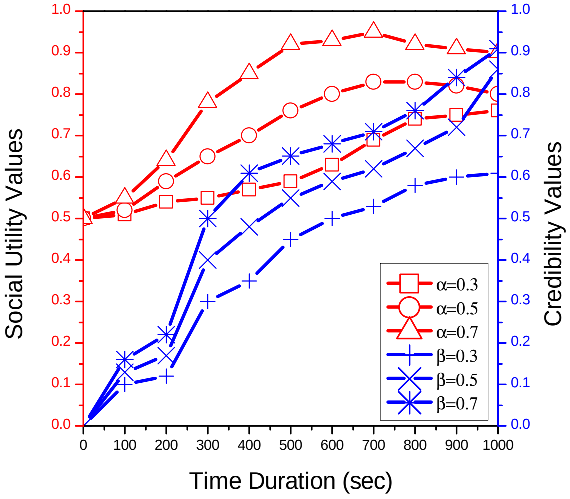


Figure 7: Effect of different values of α and β on $U^{t}_{s(i)}$ and $C^{t}_{r(i)}$ values.

behavior and social connections to achieve a trustworthy status in the VSN. To verify the accuracy of TDS, we examined the calculated trust reputation values of the nodes evolved over time against the values of initial probability of nodes under presence of 10%, 30%, 50%, and 70% malicious nodes in the network which is shown in Fig. 8. The probability density function of the initial reputation values under ideal scenario exhibits a normal distribution. We observed that at 10% and 30% malicious nodes' presence, the reputation values follow the ideal distribution very closely, which are shown in dotted lines. The Mean Square Error (MSE) values for the aforementioned scenarios are 0.0035 and 0.003 respectively which eventually converge to 0.0017 and 0.0018. Even at 50% the estimated values do not deviate significantly with MSE value of 0.004 which converges to 0.0019 eventually. Although at 70% the deviation is a little higher than that of at lower percentages having MSE value of 0.005 converging to 0.003, however it is still not a significant deviation. Moreover, it is very unlikely for a VSN to have 70% active malicious nodes at a given time. The results validate that TDS performs extremely well under the presence of a high ratio of malicious nodes.

In order to evaluate the stability of TDS we tested it for a range of 10% to 70% malicious nodes under varying conditions. In Fig. 9(a), the accuracy of high reputation based forwarder selection is shown against a range of 10%-70% malicious nodes' density in the network for a varying vehicular density

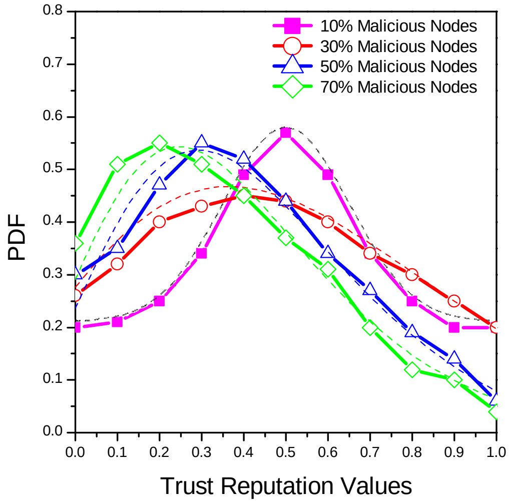
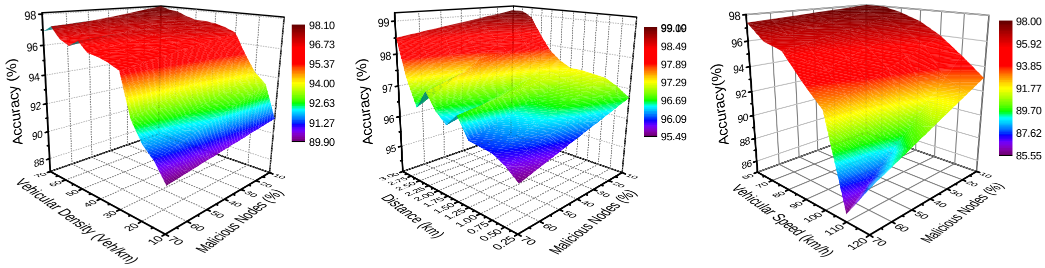


Figure 8: T_{s_i} calculated vs PDF for different percentages of malicious nodes.



(a) Effect of vehicular density on accuracy of TDS

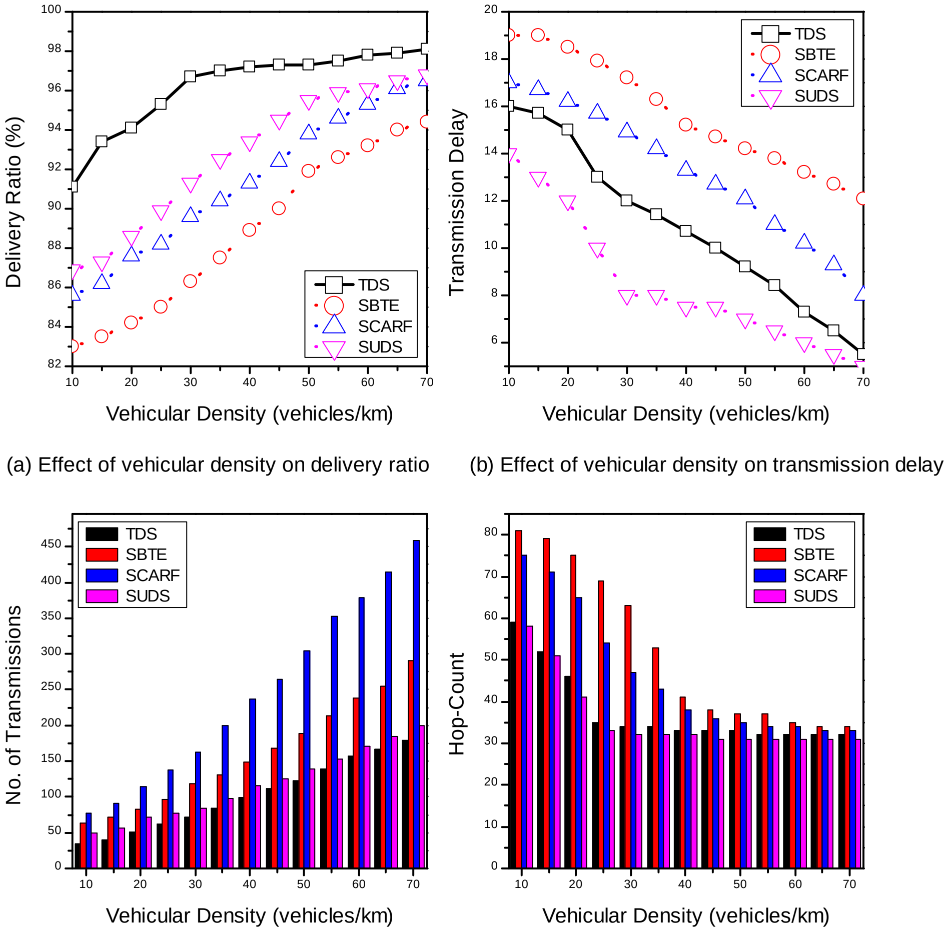
(b) Effect of varying distance on accuracy of TDS

(c) Effect of vehicular speed on accuracy of TDS

Figure 9: Performance of TDS in the presence of varying percentages of malicious nodes' density.

i.e., 10 vehicle/km to 70 vehicles/km. The results indicate that the malicious nodes' density has a very little effect on average relative accuracy of TDS, where the MSE remains relatively equal at around 2% for all values. However, a decreasing trend in the accuracy is observed at very low vehicular densities such as 10 vehicles/km and 20 vehicles/km, regardless of the malicious nodes' density. The reason behind this is the difficulty of social utility calculation in very sparse networks. Overall the accuracy of TDS remains stable for varying vehicular density.

In Fig. 9(b), the effect of varying distance on the accuracy is demonstrated. It has been observed that regardless of the malicious nodes density, the accuracy gets higher with increase in distance because of better social utility and trust score estimation. Even at very short distance of 500 meters the MSE value for high trust and reputation based selection is less than 3% while at longer distances such as 2.5 km to 3 km the MSE value is even reduced to less than 1% for the whole range of malicious nodes' density. Fig. 9(c) provides the delivery ratio of EWMs in TDS by varying vehicular speed and the percentage of malicious nodes in the network. The results indicate that smaller percentages of malicious nodes i.e., 10%-30% have negligible effect on delivery ratio at 100 km/h speed. Even at 70% of malicious nodes' presence, the performance remains quite stable at around 100 km/h speed having degraded only by 6% compared to 60 km/h. However, at speeds higher than 100 km/h the delivery ratio decreases faster for higher percentage of malicious nodes, e.g., at speed of 120 km/h, 70% of malicious nodes, the delivery ratio decrease by 9.7%. However, generally the percentage of malicious nodes is never that high in real world scenarios and so is the average speed of vehicles. Therefore, we can deduct that the performance of



(a) Effect of vehicular density on delivery ratio

(b) Effect of vehicular density on transmission delay

(c) Effect of vehicular density on No. of transmissions

(d) Effect of vehicular density on hop-count

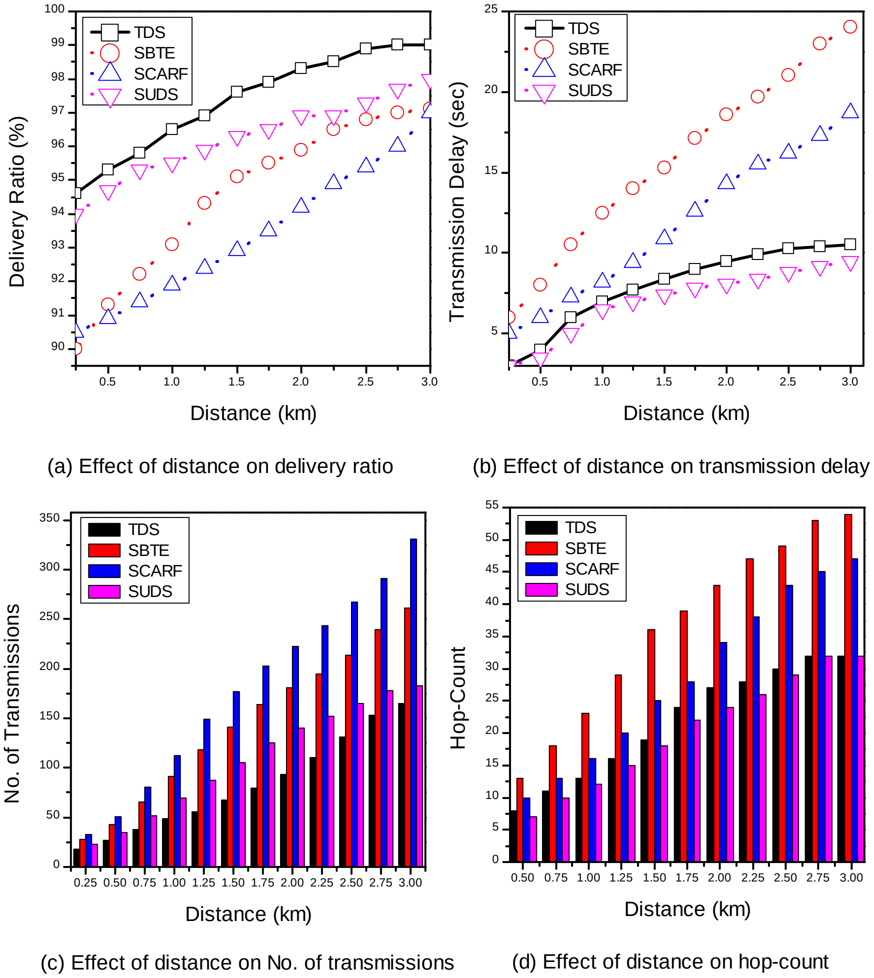
Figure 10: Comparative evaluation of TDS under varying vehicular density.

TDS remains highly stable and accurate in the presence of malicious nodes in the VSNs.

5.2.2. Comparative Analysis

Since it is evident from Fig. 9 that the performance of TDS remains extremely stable for average values of vehicular speed, density, and distance even under very high density of malicious nodes, we used a fixed value of malicious nodes density at 20% so that the performance of the aforementioned compared methods do not suffer significantly.

To analyze the scalability of TDS in comparison with the aforementioned protocols, Fig. 10 represents the performance comparison of these schemes in terms of delivery ratio, transmission delay, total number of transmissions, and hop count against varying vehicular density from 10 vehicles/km to 70 vehicles/km. The results in Fig. 10(a) indicate that in terms of delivery ratio TDS outperforms its competitors by a significant margin. For instance, at vehicular density of 70 vehicles/km, TDS delivers 37.7%, 16.3% and 13.2% higher than SBTE, SCARF, and SUDS respectively. However, at lower densities this difference gets even higher such as at 10 vehicles/km, TDS performs 88.9%, 60.3%, and 46.1% better than SBTE, SCARF, and SUDS respectively. Similarly, the variance s^2 in delivery ratio over a given range of vehicular density was recorded to be 4.51 for TDS whereas 17.38, 14.15, and 12.83 for SBTE, SCARF, and SUDS respectively, which validates the stability of TDS with varying vehicular density. Fig. 10(b) indicates the comparison in performance of these protocols in terms of transmission delay where it is evident that TDS outperforms SBTE and SCARF by a significant margin. For instance at 70% vehicular density, TDS has 50.4% and 25% lower transmission delay than SBTE and SCARF, respectively. However, it lags behind SUDS by 9% because of the reason that it takes some processing time to estimate higher trust based forwarder probability. Moreover, the variance in transmission delay is 11.92, 6.03, 8.61, and 8.43 seconds for TDS, SBTE, SCARF, and SUDS respectively with a decreasing trend for lower to higher vehicular density. This means that TDS achieves a higher rate of decrease in transmission delay compared to other protocols. From Fig. 10(c), it is evident that TDS also outperforms the other three protocols in terms of total number of transmissions of EWMs to cover the whole network with a peak value of 179 as compared to 291, 496, and 199 for SBTE, SCARF, and SUDS at 70 vehicles/km. Moreover, TDS has a standard deviation of 49.01 as compared to 74.11, 128.32, and 49.39 of SBTE, SCARF, and SUDS over the range of 10 to 70 vehicles/km. Similarly, from Fig. 10(d), we can observe that TDS requires significantly low number of hops to completely cover the whole scenario as compared to other protocols. For instance, at 10 vehicles/km the hop-count for TDS is 63 as compared to 81, 75 and 58 for SBTE, SCARF, and SUDS. At higher vehicular density such as 50-70 the difference is reduced significantly as the hop-count for all the protocols reduces. However, TDS has the lower standard deviation value of 8.79 over the whole range of vehicular density as compared to 18.73, 15.30, and 8.85 of SBTE, SCARF, and SUDS. These results validate that TDS is a scalable



(a) Effect of distance on delivery ratio

(b) Effect of distance on transmission delay

(c) Effect of distance on No. of transmissions

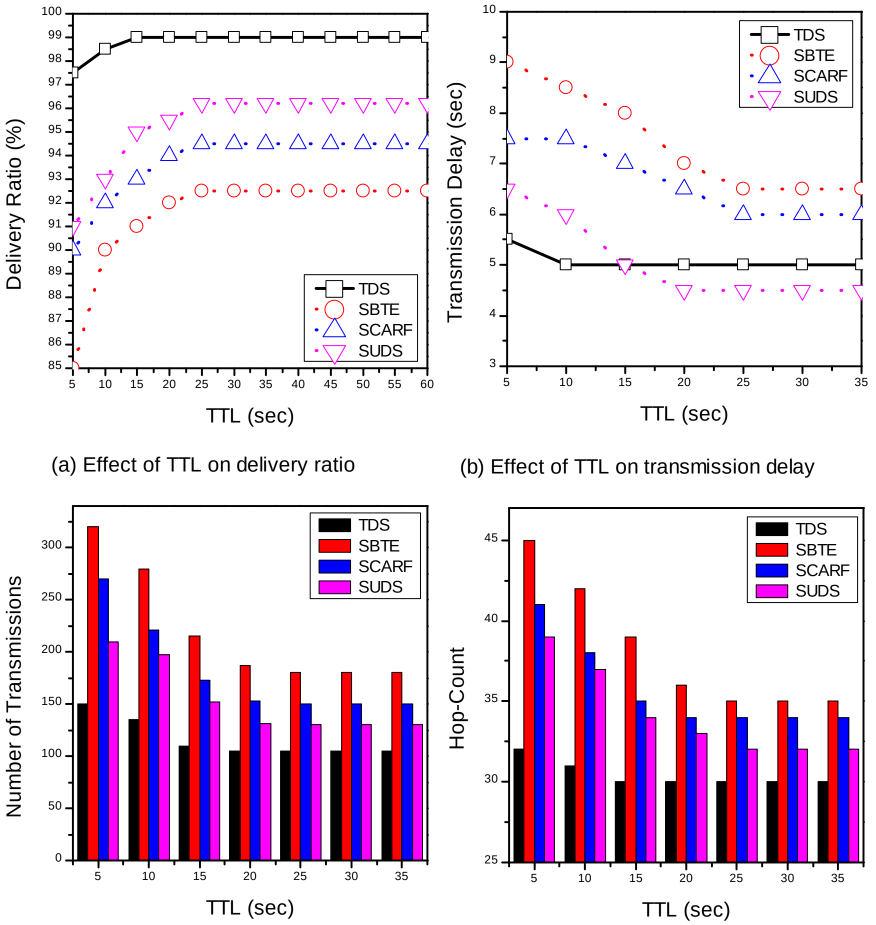
(d) Effect of distance on hop-count

Figure 11: Comparative evaluation of TDS under varying distance.

protocol and is suitable in dense and sparse networks. In order to evaluate the stability of TDS in comparison with the aforementioned protocols, Fig. 11 represents the performance comparison of these schemes over a distance of 3 kilometers on the highway. Fig. 11(a) indicates that TDS stays significantly more stable as compared to its competitors in terms of delivery ratio. This is evident from the fact that the variance in delivery ratio over 3 km was observed to be 2.32, 5.75, 4.43, and 1.47 for TDS, SBTE, SCARF, and SUDS respectively. Although variance in SUDS is lower than TDS, however, the overall delivery ratio of TDS is higher than SUDS e.g., the mean delivery ratio of TDS is 97.35% as compared to 96.25% of SUDS. Fig. 11(b) indicates the comparison of these protocols in terms of transmission delay against varying distance, where it can be observed that TDS outperforms SBTE and SCARF by a significant margin of 56.41% and 43.71% respectively at a distance of 3 km. However, it lags behind SUDS by 9.5%, because of the reason that it takes some processing time to estimate higher trust based forwarder probability to avoid false alarms. Furthermore, the variance in transmission delay is 6.40, 33.65, 21.58, 5.12 seconds for TDS, SBTE, SCARF, and SUDS respectively with a decreasing trend. Fig. 11(c) presents comparison of these protocols in terms of total number of transmissions where TDS outperforms other protocols. For instance, a peak value of 165 as compared to 261, 331, and 183 for SBTE, SCARF, and SUDS over 3 km distance. In addition, TDS has a standard deviation of 48.86 compared to 76.91, 96.67, and 56.06 of SBTE, SCARF, and SUDS over a range of 0.25-3 km. In Fig. 11(d), it can be noted that TDS remains significantly stable with fewer number of next hop broadcasters as compared to SBTE and SCARF while SUDS almost matches it as the distance increases. From the variance of hop-count over range of 0.25-3km, which is 77.16, 202.61, 176.6, and 78.25 for TDS, SBTE, SCARF, and SUDS respectively, it can be noted that TDS stays relatively stable with significantly lower rate of increase than all the others. These findings indicate that TDS performs with high stability over long distances.

In Fig. 12, we demonstrate the effect of varying TTL on the performance of TDS and other protocols under constant vehicular density, speed, and distance. Fig. 12.(a), (c), and (d) show that TDS outperforms other protocols by significant margins in terms of delivery ratio, total number of transmissions and hop-count. For instance, the delivery ratio of TDS is almost 7%, 8% and 13% higher than that of SUDS, SCARF, and SBTE respectively for TTL set at 5 seconds. It is worth noting that the performance of TDS remains almost constant beyond TTL value of 10 while others fluctuate and achieve steady results beyond TTL set at 25 seconds. Similarly, Fig. 12(c) demonstrates that at lower values of TTL, TDS disseminates approximately 21%, 45%, and 54 % less number of messages as compared to SUDS, SCARF, and SBTE respectively. In Fig. 12(b), we can also observe that over all TTL values, TDS outperforms its competitors by a significant margin. However, initially TDS performs better than SUDS in terms of transmission delay, but after TTL set at 10 seconds, SUDS achieves approximately 0.5 seconds faster delivery while the others remain relatively much higher than them. Overall the performance of TDS remains almost constant beyond TTL value of 5 seconds as compared to others. As TTL increases, the message remains for a longer time in the buffer because the protocols consume longer time to select suitable broadcasters and hence the increase in delay and number of transmissions.

As vehicles are high mobility nodes especially in a highway scenario, their speed has a direct impact on the performance of networking protocols. Therefore the robustness of a protocol can be evaluated by testing it over a range of speed. For this reason, Fig. 13 represents the performance comparison of TDS with the aforementioned schemes by varying the vehicular speed from



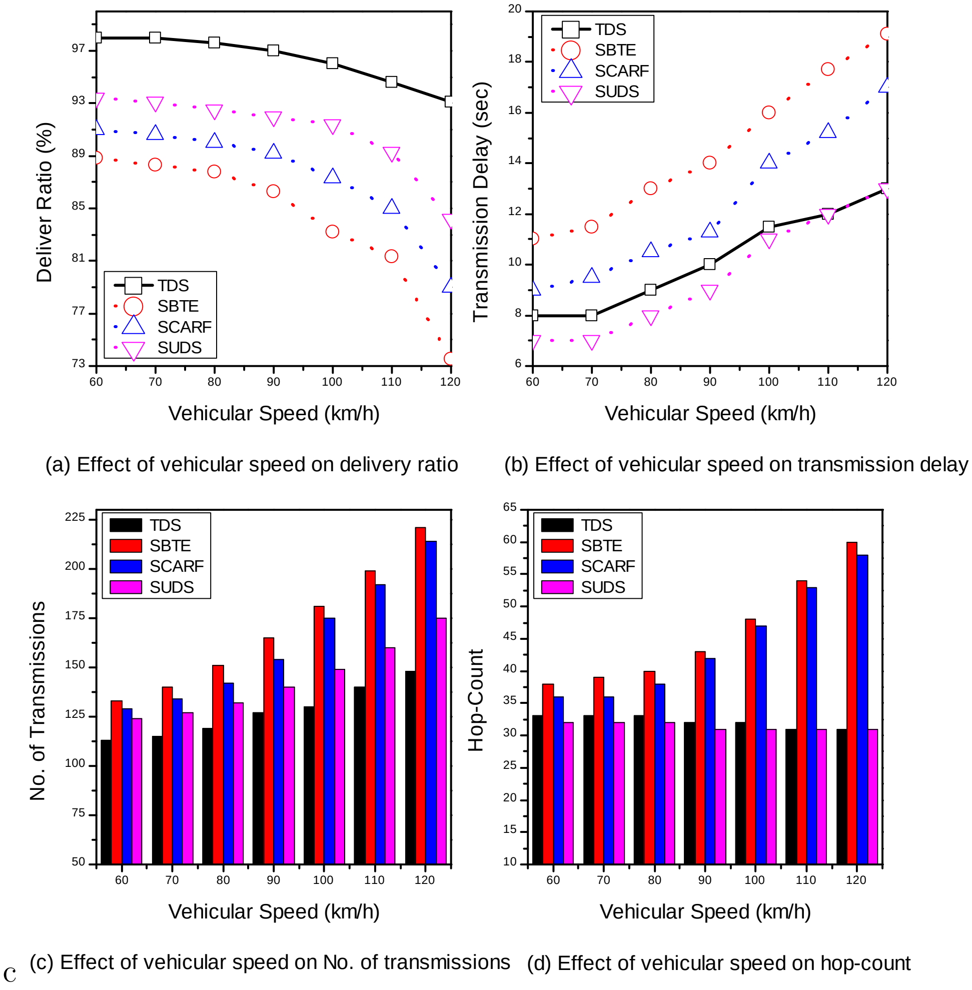
(a) Effect of TTL on delivery ratio

(b) Effect of TTL on transmission delay

(c) Effect of TTL on No. of transmissions

(d) Effect of TTL on hop-count

Figure 12: Comparative evaluation of TDS under varying TTL.



(a) Effect of vehicular speed on delivery ratio

(b) Effect of vehicular speed on transmission delay

(c) Effect of vehicular speed on No. of transmissions

(d) Effect of vehicular speed on hop-count

Figure 13: Comparative evaluation of TDS under varying vehicular speed.

60 km/h up to 120 km/h. Fig. 13(a) shows their comparison in terms of delivery ratio, where TDS performs significantly well having a variance of 3.52, as compared to 29.87, 18.25, and 10.42 of SBTE, SCARF, and SUDS respectively. Similarly, at speed of 60 km/h TDS performs 93.7%, 71.42%, and 46.1% better than SBTE, SCARF, and SUDS respectively. At higher speeds this gap further increases such that at 120 km/h TDS performs 210%, 151%, and 95% better than SBTE, SCARF, and SUDS respectively. In Fig. 13(b), transmission delay for all protocols is compared against increasing speed. Although TDS lags behind SUDS initially at lower speeds such as at

60-90 km/h by 1 second, it catches up at higher speed with SUDS whereas outperforming SBTE and SCARF by a significant margin of about 272% and 111% at 60 km/h while 319% and 235% at 120 km/h. It is worth noting that the effect of vehicular speed on TDS is much smaller than it has on the other three protocols. This can be noted from the variance of transmission delay which is 3.90, 9.55, 9.38, and 5.95 for TDS, SBTE, SCARF, and SUDS respectively. Fig. 13(c) and Fig. 13(d) compare these protocols in terms of total number of transmissions and hop-count respectively. In both cases TDS has a lower count than the others. The lower standard deviation value i.e., 13.04 for TDS as compared to 32.19, 31.89, 18.66 for the other three respectively indicates that it is less affected by speed than the others. Similar is the case in hop-count in comparison with the former two while SUDS initially has a 3% lower value than that of TDS but TDS catches up with SUDS. However, vehicular speed is relatively higher than 80 km/h on highways which undermines the negligible difference in hop-count between TDS and SUDS at lower speeds. These results validate that TDS is a robust, stable and scalable dissemination protocol as compared to the aforementioned protocols.

The reasons for better performance of TDS compared to the aforementioned methods which is evident from the above analysis are manifold. Firstly, TDS employs the hybrid architecture of VSNs which ensures uninterrupted connectivity of the nodes in order to disseminate the EWMs in the network with extremely high delivery ratio. Secondly, the percolation centrality metric can capture the change in social features more dynamically in highly dynamic environments such as VSNs as compared to other centrality metrics that are used in the aforementioned methods. Therefore, the selection of broadcaster in each iteration is more accurate resulting in lower transmission delay, number of transmissions, and hop-count. Moreover, selection of higher reputation based nodes narrows down the total number of suitable broadcasters and reduces the chance of message replication which ensures the avoidance of broadcast storm problem and network congestion. Similarly, the proposed mechanism regularly updates the social metrics and reputation of the nodes which are carried intrinsically over the time, therefore it requires significantly less time to initiate the dissemination process and hence operates even at very low TTL values. Although there is very marginal amount of extra transmission delay as compared to SUDS at the cost of authentic message delivery which the later does not ensure but it is not very significantly high and almost negligible at the average values of the measuring parameters.

6. Conclusion

To solve the problem of fake emergency warning messages generated by malicious nodes, we proposed a trust based dissemination scheme for authentic EWMs in VSNs. We first evaluated the nature of EWM by employing a user-post interaction network to identify whether a generated EWM is true or fake. Then to disseminate a true EWM in the whole network, first we developed a mechanism where nodes build reputation, based on their behavior contribution in their social networks, and social activity over a longer period of time. Based on the reputation and social importance of the node we estimated a trust-score for each node. Moreover, we calculated a social-utility for each node based on its centrality, social interactions, and similarity with other nodes which is used in conjunction with trust-score to select a broadcaster. In order to disseminate EWMs, we employed V2I based strategy via social groups in case of infrastructure availability while V2V based strategy via friendship networks of the nodes in the absence of infrastructure support.

To analyze the performance and accuracy of TDS, performed extensive experiments for various network parameters and compared it against the state-of-the-art schemes in VSNs. The results indicate that TDS outperforms its competitors in terms of the aforementioned parameters by significant margins, however it lags behind SUDS very marginally in terms of transmission delay at the cost of trustworthiness and authenticity of the EWMs. In future we plan to extend our work to investigate problems such as, effect of selfish behavior of nodes on the dissemination of EWMs. Moreover, we will explore the possibilities of EWMs dissemination in urban scenario which is very much different than highways and its network structure poses varied challenges.

Acknowledgements

The authors extend their appreciation to the International Scientific Partnership Program ISPP at King Saud University for funding this research work through ISPP-78. This work is partially supported by National Natural Science Foundation of China under Grant No.61572106 and No. 61971084, Dalian Science and Technology Innovation Fund under Grant No. 2018J12GX048, Fundamental Research Funds for the Central Universities under Grant No.

DUT19JC18 and Grant No. DUT18JC09, National Natural Science Foundation of Chongqing under Grant cstc2019jcyj-msxmX0208, and open research fund of National Mobile Communications Research Laboratory, Southeast University under Grant No.2020D05.

References

[1] S. Latif, S. Mahfooz, B. Jan, N. Ahmad, Y. Cao, M. Asif, A comparative study of scenario-driven multi-hop broadcast protocols for vanets, Veh. Commun. 12 (2018) 88–109. doi:https://doi.org/10.1016/j.vehcom.2018.01.009.

[2] A. Mchergui, T. Moulahi, B. Alaya, S. Nasri, A survey and comparative study of qos aware broadcasting techniques in vanet, Telecommun. Syst. 66 (2) (2017) 253–281. doi:10.1007/s11235-017-0280-9.

[3] F. Xia, L. Liu, J. Li, J. Ma, A. V. Vasilakos, Socially aware networking: A survey, IEEE Syst. J. 9 (3) (2015) 904–921. doi:10.1109/JSYST.2013.2281262.

[4] Z. Ning, L. Liu, F. Xia, B. Jedari, I. Lee, W. Zhang, Cais: A copy adjustable incentive scheme in community-based socially aware networking, IEEE Transactions on Vehicular Technology 66 (4) (2017) 3406–3419.

[5] X. Wang, Z. Ning, L. Wang, Offloading in internet of vehicles: A fog-enabled real-time traffic management system, IEEE Transactions on Industrial Informatics 14 (10) (2018) 4568–4578.

[6] Q. Xu, Z. Su, K. Zhang, P. Ren, X. S. Shen, Epidemic information dissemination in mobile social networks with opportunistic links, IEEE Trans. Emerg. Top. Comput. 3 (3) (2015) 399–409. doi:10.1109/TETC.2015.2414792.

[7] Z. Ning, X. Hu, Z. Chen, M. Zhou, B. Hu, J. Cheng, M. S. Obaidat, A cooperative quality-aware service access system for social internet of vehicles, IEEE Internet of Things Journal 5 (4) (2017) 2506–2517.

[8] A. Rahim, X. Kong, F. Xia, Z. Ning, N. Ullah, J. Wang, S. K. Das, Vehicular social networks: A survey, Pervasive Mob. Comput. 43 (2018) 96–113. doi:https://doi.org/10.1016/j.pmcj.2017.12.004.

[9] K. M. Alam, M. Saini, A. E. Saddik, Toward social internet of vehicles: Concept, architecture, and applications, IEEE Access 3 (2015) 343–357. doi:10.1109/ACCESS.2015.2416657.

[10] Z. Ning, F. Xia, N. Ullah, X. Kong, X. Hu, Vehicular social networks: Enabling smart mobility, IEEE Commun. Mag. 55 (5) (2017) 49–55. doi:10.1109/MCOM.2017.1600263.

[11] Z. Ning, J. Huang, X. Wang, J. J. P. C. Rodrigues, L. Guo, Mobile edge computing-enabled internet of vehicles: Toward energy-efficient scheduling, IEEE Network 33 (5) (2019) 198–205.

[12] N. Ullah, X. Kong, L. Wan, H. Chen, Z. Wang, F. Xia, A social utility-based dissemination scheme for emergency warning messages in vehicular social networks, Comput. J. 61 (7) (2018) 971–986. doi:10.1093/comjnl/bxy026.

[13] Z. Ning, P. Dong, X. Wang, M. S. Obaidat, X. Hu, L. Guo, Y. Guo, J. Huang, B. Hu, Y. Li, When deep reinforcement learning meets 5g-enabled vehicular networks: A distributed offloading framework for traffic big data, IEEE Transactions on Industrial Informatics 16 (2) (2020) 1352–1361.

[14] J. Lee, J. C. Oh, A model for recursive propagations of reputations in social networks, in: Proc. ASONAM ?3, Niagra Falls, ON, Canada, 2013, pp. 666–670. doi:10.1109/ASONAM.2013.6785774.

[15] W. Li, H. Song, Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 17 (4) (2016) 960–969. doi:10.1109/TITS.2015.2494017.

[16] T. Biswas, A. Sanzgiri, S. Upadhyaya, Building long term trust in vehicular networks, in: Proc. VTC Spring, Nanjing, China, 2016, pp. 1–5. doi:10.1109/VTCSpring.2016.7504149.

[17] A. M. Vegni, V. Loscri, R. Petrolo, Scarf: A social-aware reliable forwarding technique for vehicular communications, in: Proc. SMARTOBJECTS '17, Snowbird, Utah, USA, 2017, pp. 1–6. doi:10.1145/3127502.3127512.

[18] D. Alishev, R. Hussain, W. Nawaz, J. Lee, Social-aware bootstrapping and trust establishing mechanism for vehicular social networks, in: Proc. VTC Spring, Sydney, NSW, Australia, 2017, pp. 1–5. doi:10.1109/VTCSpring.2017.8108459.

[19] W. Moreira, P. Mendes, Social-aware forwarding in opportunistic wireless networks: Content awareness or obliviousness?, in: Proc. WoWMoM 2014, Sydney, NSW, Australia, 2014, pp. 1–6. doi:10.1109/WoWMoM.2014.6918915.

[20] H. Gong, L. Yu, X. Zhang, Social contribution-based routing protocol for vehicular network with selfish nodes, Int. J. Distrib. Sens. Networks 10 (4). arXiv:https://doi.org/10.1155/2014/753024, doi:10.1155/2014/753024.

[21] F. Xia, L. Liu, B. Jedari, S. K. Das, Pis: A multi-dimensional routing protocol for socially-aware networking, IEEE Transactions on Mobile Computing 15 (11) (2016) 2825–2836. doi:10.1109/TMC.2016.2517649.

[22] A. Rahim, T. Qiu, Z. Ning, J. Wang, N. Ullah, A. Tolba, F. Xia, Social acquaintance based routing in vehicular social networks, Futur. Gener. Comput. Syst.doi:https://doi.org/10.1016/j.future.2017.07.059.

[23] X. Chen, C. Shang, B. Wong, W. Li, S. Oh, Efficient multicast algorithms in opportunistic mobile social networks using community and social features, Comput. Networks 111 (2016) 71–81. doi:https://doi.org/10.1016/j.comnet.2016.07.007.

[24] H. Zhu, M. Dong, S. Chang, Y. Zhu, M. Li, X. S. Shen, Zoom: Scaling the mobility for fast opportunistic forwarding in vehicular networks, in: Proc. INFOCOM 2013, Turin, Italy, 2013, pp. 2832–2840. doi:10.1109/INFCOM.2013.6567093.

[25] F. Xia, A. M. Ahmed, L. T. Yang, J. Ma, J. J. P. C. Rodrigues, Exploiting social relationship to enable efficient replica allocation in ad-hoc social networks, IEEE Trans. Parallel Distrib. Syst. 25 (12) (2014) 3167–3176. doi:10.1109/TPDS.2013.2295805.

[26] F. Xia, A. M. Ahmed, L. T. Yang, Z. Luo, Community-based event dissemination with optimal load balancing, IEEE Trans. Comput. 64 (7) (2015) 1857–1869. doi:10.1109/TC.2014.2345409.

[27] L. A. Maglaras, D. Katsaros, Social clustering of vehicles based on semi-markov processes, IEEE Trans. Veh. Technol. 65 (1) (2016) 318–332. doi:10.1109/TVT.2015.2394367.

[28] X. Kong, F. Xia, Z. Ning, A. Rahim, Y. Cai, Z. Gao, J. Ma, Mobility dataset generation for vehicular social networks based on floating car data, IEEE Trans. Veh. Technol. 67 (5) (2018) 3874–3886. doi:10.1109/TVT.2017.2788441.

[29] F. Xia, A. Rahim, X. Kong, M. Wang, Y. Cai, J. Wang, Modeling and analysis of large-scale urban mobility for green transportation, IEEE Trans. Ind. Informat. 14 (4) (2018) 1469–1481. doi:10.1109/TII.2017.2785383.

[30] Z. Ning, F. Xia, X. Hu, Z. Chen, M. S. Obaidat, Social-oriented adaptive transmission in opportunistic internet of smartphones, IEEE transactions on Industrial Informatics 13 (2) (2017) 810–820.

[31] F. D. Cunha, G. G. Maria, A. C. Viana, R. A. Mini, L. A. Villas, A. A. Loureiro, Socially inspired data dissemination for vehicular ad hoc networks, in: Proc. MSWiM '14, Montreal, QC, Canada, 2014, pp. 81–85. doi:10.1145/2641798.2641834.

[32] A. Dua, N. Kumar, S. Bawa, Reidd: Reliability-aware intelligent data dissemination protocol for broadcast storm problem in vehicular ad hoc networks, Telecommun. Syst. 64 (3) (2017) 439–458. doi:10.1007/s11235-016-0184-0.

[33] Q. Yang, H. Wang, Toward trustworthy vehicular social networks, IEEE Commun. Mag. 53 (8) (2015) 42–47. doi:10.1109/MCOM.2015.7180506.

[34] T. N. D. Pham, C. K. Yeo, Adaptive trust and privacy management framework for vehicular networks, Veh. Commun. 13 (2018) 1–12. doi:https://doi.org/10.1016/j.vehcom.2018.04.006.

[35] F. Xia, B. Jedari, L. T. Yang, J. Ma, R. Huang, A signaling game for uncertain data delivery in selfish mobile social networks, IEEE Trans. Comput. Social Syst. 3 (2) (2016) 100–112. doi:10.1109/TCSS.2016.2584103.

[36] X. Chen, L. Wang, A trust evaluation framework using in a vehicular social environment, in: Proc. INFOCOM WKSHPS, Atlanta, GA, USA, 2017, pp. 1004–1005. doi:10.1109/INFCOMW.2017.8116532.

[37] B. Lin, X. Chen, L. Wang, A cloud-based trust evaluation scheme using a vehicular social network environment, in: Proc. APSEC '17, Nanjing, China, 2017, pp. 120–129. doi:10.1109/APSEC.2017.18.

[38] Z. Wang, X. Pang, Y. Chen, H. Shao, Q. Wang, L. Wu, H. Chen, H. Qi, Privacy-preserving crowd-sourced statistical data publishing with an untrusted server, IEEE Trans. Mobile Comput. (2018) 1–1doi:10.1109/TMC.2018.2861765.

[39] B. Jedari, L. Liu, T. Qiu, A. Rahim, F. Xia, A game-theoretic incentive scheme for social-aware routing in selfish mobile social networks, Futur. Gener. Comput. Syst. 70 (2017) 178–190. doi:https://doi.org/10.1016/j.future.2016.06.020.

[40] K. Shu, S. Wang, H. Liu, Understanding user profiles on social media for fake news detection, in: Proc. MIPR, Miami, FL, USA, 2018, pp. 430–435. doi:10.1109/MIPR.2018.00092.

[41] Z. Jin, J. Cao, Y. Zhang, J. Luo, News verification by exploiting conflicting social viewpoints in microblogs, in: Proc. AAAI '16, Phoenix, AZ, USA, 2016, pp. 2972–2978.

[42] M. Piraveenan, M. Prokopenko, L. Hossain, Percolation centrality: Quantifying graph-theoretic impact of nodes during percolation in networks, PLOS ONE 8 (1) (2013) 1–14. doi:10.1371/journal.pone.0053095.

[43] J. Li, Z. Ning, B. Jedari, F. Xia, I. Lee, A. Tolba, Geo-social distance-based data dissemination for socially aware networking, IEEE Access 4 (2016) 1444–1453. doi:10.1109/ACCESS.2016.2553698.

[44] L. Gao, M. Li, A. Bonti, W. Zhou, S. Yu, Multidimensional routing protocol in human-associated delay-tolerant networks, IEEE Trans. Mob. Comput. 12 (11) (2013) 2132–2144. doi:10.1109/TMC.2012.188.

[45] R. I. Ciobanu, C. Dobre, Crawdad dataset upb/hyccups (v. 2016-10-17), Downloaded from https://crawdad.org/upb/hyccups/20161017 (oct 2016). doi:10.15783/C7TG7K.

[46] X. Fan, L. Liu, M. Li, Z. Su, Eigentrustp++: Attack resilient trust management, in: Proc. CollaborateCom, Pittsburg, PA, USA, 2012, pp. 416–425.

[47] R. Cabaniss, S. S. Vulli, S. Madria, Social group detection based routing in delay tolerant networks, Wirel. Netw. 19 (8) (2013) 1979–1993. doi:10.1007/s11276-013-0580-2.