TACASHI: Trust-Aware Communication Architecture for Social internet of veHIcles with human factor consideration

Chaker Abdelaziz Kerrache, Abderrahim Benslimane, Nasreddine Lagraa, Carlos T. Calafate, Juan-Carlos Cano, Anna Maria Vegni, and Rasheed Hussain

***Abstract*—Internet of Vehicles (IoVs) is evolving as a new theme of research and development from vehicular ad hoc networks (VANETs). Unlike VANETs, IoVs is composed of smart objects equipped with a powerful multi-sensor platform, communications technologies, computation units, IP-based connectivity to the Internet and to other vehicles creating as a result a social network called Social IoVs (SIoVs). Ensuring the required trustiness among communicating peers is an important task in such heterogeneous networks, especially for safety-related applications where the margin of error is extremely undesired. Most the safety applications are a kind of decision aided system, and final decision is always taken by humans. Thus, in addition to securing inter-vehicle communication, the driver/passengers honesty factor must be also considered. With the appearance of 5G technology it became possible to connect SIoVs to any other network including Online Social Networks (OSNs). In this paper, we took advantage of this possibility to connect SIoVs and OSN, for the purpose of estimating the drivers and passengers honesty based on their OSN profiles. Furthermore, we also compare the current vehicles location with their estimated path based on their historical movement. Events such as soccer games, festivities, and emergency cases are also taken into account the path estimation. Afterward, we combined the SIoV, path-based and OSN-based trusts to compute the overall trust about the different vehicles and their drivers/passengers. As result, our proposal called TAKASHI offers a trust-aware social In-vehicle and inter-vehicle communication architecture for SIoVs considering also the human honesty factor based of Online Social Networks. Conducted simulation show that.....**

***Index Terms*—TAKASHI; VANET; Social Internet of Vehicles; Human factor; Trust.**

I. Introduction

Vehicular Adhoc Networks (VANETs) are considered as a main component of the Cooperative Intelligent Transportation Systems (C-ITS). Various kinds of applications came up with the appearance of these networks, most of them based on inter-vehicle communication [1]. Furthermore, many of these applications represent a decision-aided system. Hence, the final decision will be taken by a human being, and the system has no idea about how honest is this person.

In VANET, a vehicle is mainly considered as a node to disseminate messages among vehicles. In the IoV paradigm, each vehicle is considered as a smart object equipped with a powerful multi-sensor platform, communications technologies, computation units, IP-based connectivity to the Internet and to other vehicles either directly or indirectly [2]. In addition, a vehicle in IoV is envisioned as a multi-communication model, enabling the interactions between intra-vehicle components, vehicles and vehicles, vehicles and road, and vehicles and people. IoV enables the acquistion and processing of large amount of data from versatile geographical areas via intelligent vehicles computing platforms to offer various categories of services for road safety and other services to drivers and passengers [3].

Furthermore, Social Internet of Vehicles (SIoVs) are a subset of socially-aware networks [4]–[6]. They took advantage of the shared applications, destinations, or target to build up a temporal social community among vehicles. Besides, this social aspect of the vehicles is also the base of fully distributed vehicular cloud [7]. On the other hand, with the appearance of 5G technology accessing all internet service can be done anytime and anywhere [8]. In addition, vehicles path can be easily estimated through the use its historical moving paths and its driver's social interactions and hobbies. For example, a daily worker would likely go every day at 8am to work and comeback home at 5pm out of weekends and holidays, if his car is being detected in a different far location the SIoV system can trigger a possible stolen vehicle alert an alert or for instance, text the vehicle's owner.

Relying on the assumption that all passengers and vehicles are honest and collaborative can lead to undesired situation. For instance, EYES application [9] is a decision-aided overtaking system helping the driver to take the right decision. Thus, SIoV security together with the passengers'honesty must be taken into account in designing a global SIoV communication system [10], [11].

Many solutions have been proposed to secure inter-vehicle communication, and they are generally classified into cryptography-based [12], trust-based [13], [14], these latters are known to be less energy and time consuming compared to the cryptography-based ones. However, there was also some

C.A. Kerrache is with the Department of Mathematics and computer science, University of Ghardaia, Algeria, Emai: ch.kerrache@lagh-univ.dz

A. Benslimane is with University of Avigon, Email: abderrahim.benslimane@univ-avignon.fr

A.M. Vegni is Department of Engineering, Roma Tre University, 00146 Rome, Italy Emai: annamaria.vegni@uniroma3.it

A. Benslimane is with University of Avigon, Email: abderrahim.benslimane@univ-avignon.fr

C.T. Calafate, J.C. Cano, and P. Manzoni are with Department of Computer Engineering, Universitat Politècnica de València, Camino de Vera, S/N, Valencia, Spain E-mail: {calafate,jucano}@disca.upv.es

R. Hussain and J. Lee are with the Institute of Information Systems, Innopolis University, Innopolis, Russia. E-mail: {r.hussain,j.lee}@innopolis.ru

C.A. Kerrache is the corresponding author.

works combining both types pf solutions [15], [16].

In this paper, we propose a novel SIoV communication architecture that takes advantage of Online Social Networks (OSNs) to enhance the SIoV trust establishment by the human and location-related honesty consideration. We used the group-trust metric adopted by Advogato[1] attempting to determine the maximum set of trusted peers while minimizing the influence of unreliable dishonest peers [17]. Afterwards, an honesty-related classification (good, bad, or compromised) is associated to every node (driver/passenger) and vehicle location depending on the Advogato classification of this node (either trusted or distrusted) and the location tracking system respectively.

Simultaneously, the inter-vehicle trust is also estimated, then combined with the RSUs and Trusted Authorities recommendations. Finally, the Advogato results are also used to identify honest and dihonest drivers/passengers. Using this strategy, the aim is not just to reduce both the detection errors ratios and also the ratio of doubtful nodes that the inter-vehicle trust could not classify the to either trusted or distrusted peers, but also to prevent unwanted situations such as stolen vehicles.

The rest of this paper is organized as follows: in section II, we present some background in VANET, IoV, VSNs, OSNs, and trust establishment in both kind of networks. Afterward, in section III, we present an overview of our proposal, followed by its details in section IV. TAKASHI's dishonesty detection process is the discussed in section V. Before concluding our paper in sectionVII, we describe in section VI our simulation environment followed by the discussion the obtained results.

II. State of the art

Various solutions have adopted trust modeling to enhance the inter-vehicle communication for VANET, Social VANET, IoV, and SIoV context. We hover in this section the main features of the socially-aware networking as well as the existing trust-based solutions in these domains.

A. Social trust and socially-aware networking

The proliferation of handheld devices requires mobile carriers to provide instant connectivity. Moreover, the movements of the users is generally related to their social behaviors and relationships, and the mobility patterns of mobile devices carried by these users are strongly depend on their movements. Thus, mobile networks nowadays are more and more human centric. As result, the new field called socially-aware networking (SAN) has emerged [18]. This new paradigm of social-awareness is applicable to many types of inter-node interaction-based networks such as ad hoc networks, mobile social networks, opportunistic networks). By taking advantage of nodes' social properties, Socially Aware Networks can present better networking platform to new applications and services. Furthermore, it makes easy the convergence of human society and cyberphysical systems.

Figure 1 represents a global overview of socially-aware networking concepts and its different layers. For our case we focus mainly on the red rectangle representing security and privacy protocols using online networks.

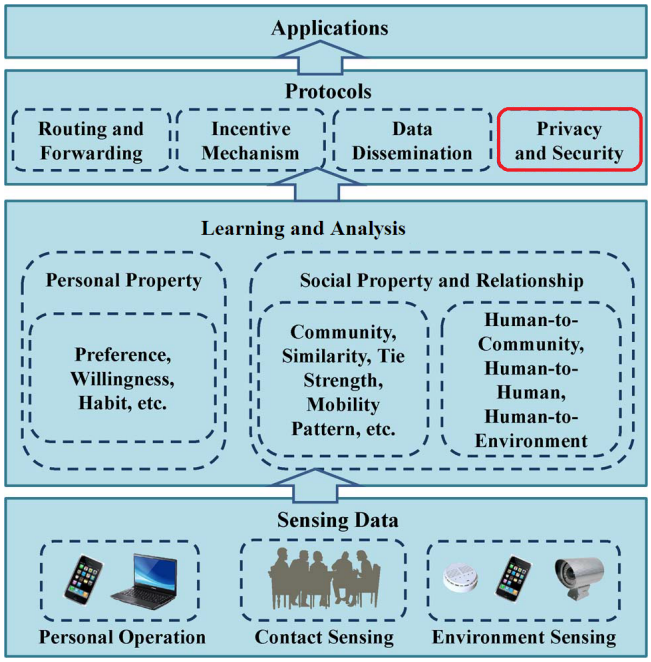

Fig. 1: Socially-aware networking overview.

Notice that introducing online social networks in VANETs differs from the vehicular social networks approach where a set of vehicles located in the same geographical area, and typically going to the same destinations, can share some application, purposes, or services, thereby forming a temporal inter-vehicle social network.

B. Trust in Online Social Networks (OSNs)

As mentioned above, trust establishment has proved its efficiency at enhancing the security of different types of networks. Many proposals have been developed for OSNs as well [19], [20]. The general trust establishment proposals for OSNs are based either on the Advogato trust metric [17], or PageRank solutions [21].

Besides the graph-based logical structure of OSNs, figure 2 summarizes the application-oriented structure of trust establishment in Online social networks. Generally, trust for OSNs can be classified using three complementary phases: (i) trust information collection, (ii) trust evaluation, and (iii) trust information dissemination. To identify how honest and trustful is a profile owner, social trust is based on a scalar estimation using the personal profile information, which includes user identity and interactions with other users. Once this social trust is estimated, it will be provided to the end users in different manners and for different purposes.

C. Trust in VANET and Internet of Vehicles (IoV)

In VANET context, trust management schemes are generally classified as entity-based, data-based, and hybrid models following the targeted adversary which can be dishonest entities, malicious messages, or both [13], [22].

[1] http://www.advogato.org/

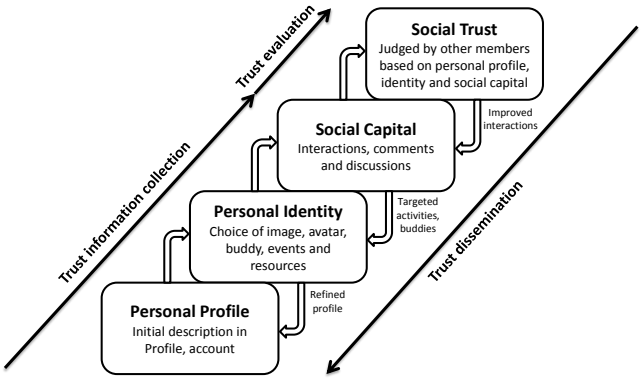

Fig. 2: Trust establishment in OSNs.

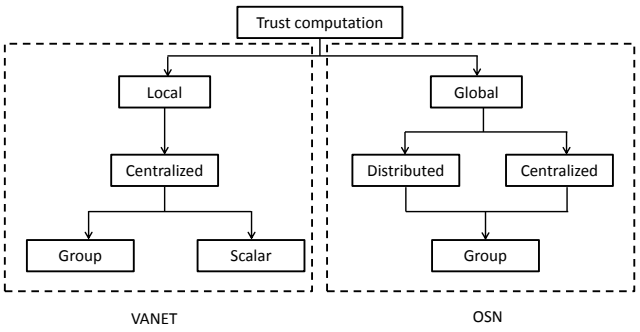

Fig. 3: VANET trust vs OSN trust.

Works in [23], [24] represent entity-based trust models, authors of [23] try to revoke nodes by sending falsified messages and fake information, respectively, using different techniques. Haddadou et al. [24] chose to associate a credit value to each neighbor vehicle which will increase or decrease depending on the concerned neighbor's messages credibility. Hence, this credit will be quickly decreased when replaying or injecting new messages.

As for the data-based approaches, Gurung et al. [25] adopted three metrics to classify received messages into either legal or malicious messages; these metrics are content similarity, content conflict, and routing path similarity. However, in addition to its high time complexity, this solution does not take into account the high level of mobility associated to VANETs, nor the case of node sparsity.

Our previous hybrid models [26], [27] focus mainly on facing Denial of service and coalition attacks in VANETs using the standardized messaging service. However, the additional traffic generated by the recommendation requests/responses might affect some safety-related applications.

On the other hand, few solutions addressing trust issues is IoV have been recently published [28].

In [29] authors propose a trust-aware cluster-based anomaly detection scheme for intelligent vehicles, this proposal modifies the Affinity Propagation Clustering technique to generate the most trustworthy cluster head based on the inter-vehicle communications. They also adopt an RSU-enhanced reputation provision scheme where a Central Arbitrator (CA) collects evidences from sparse RSUs. Then, a reputation system is established to evaluate global and history reputation from accumulated data. While ensuring a reduced error ratios in detecting malicious vehicles, the whole detection process is an infrastructure-based process. However, this cannot be always insured in highly dynamic environment like IoV.

Hussain et al. [30] proposed a trust model collecting evidence from IoV infrastructures then store them in vehicles Tamper-Proof Devices (TPD), then start inter-vehicle trust-based communication. The main limitation of this approaches is the fact that vehicles behaviour may change. Thus, store trust information should not be static over time. In addition, authors did not evaluate the performance in a realistic environment implementing the different VANETs low layers features.

Unlike the existing trust models, Gai et al. [31] propose a Trust Management system for SIoV called RTM where each node stores its own reputation information rated by others during past transactions. They introduced a CA server is to ensure the integrality and the undeniability of the trust information. However, besides the additional cost of the introduced server, this scheme does not work in rural scenario or low density cases, and same as all existing proposals, the human honesty factor is not considered.

D. Trust computation in Vehicular Networks and Online Social Networks

Establishing trust in any network involves the inheritance of this network's features. Therefore, due to the distributed nature of vehicular networks, every vehicle locally evaluates its neighbors trustiness. This trust computation can be done either in a scalar way, using the piggybacked opinions within exchanged messages, or through clustered and group-based collaboration among vehicles located in a same area [13]. Differently from this situation, trust in online social networks requires having a sink or a third trusted party that is responsible for evaluating the different peers. This sink can either handle the whole task of trust computation, or it can distribute such task among secondary sinks, which are typically community leaders. Hence, by introducing the community context, trust computation is now based on a group instead of scalar information [4]. Figure 3 summarizes the difference between VANET and OSN trust computations.

III. TACASHI Overview

Establishing SIoV trut with the incorporation of the human honesty factor should be achieved by relying on third trusted authorities as intermediaries for this information, since the latter are the only ones having the possibility to trace/track vehicles identity together with their drivers/owners. Accounting for the vehicles' identity is not a problem as every vehicle should have a valid certificate and a set of pseudonyms provided by the trusted authority. However, matching the driver identity and social account with the vehicle identity

involves the use of other intermediate tools such as digital fingerprint, eyes and voice recognition systems, or a subscriber identification module (SIM), thus imposing more requirements onto the system.

Due to the high cost of smart vehicles, and to the probable lack of RSUs in rural environments, Android-based platforms including smartphones and tablets have recently emerged as an alternative solution to provide vehicular communications[2]. This way, any trusted third authority can be reached using different cellular network technologies. This new research area is know as Heterogeneous Vehicular Networking [32].

Figure 4 represents an overview of our proposed SIoV architecture in which, besides passengers, vehicles,roadside units, and trusted authorities we also involve online social networks. These latter are accessed through a trusted middelware such as network operator, RSUs, or Trusted Authorities like city hall.

A. TACASHI Actors

TAKASHI architecture involves five main actors which are the person registered as the vehicle owner, the passengers within the vehicle represented by their connected devices, the vehicles themselves, RoadSide Units and Trusted authorities, and the Online Social Network accounts connected to the driver and passengers devices. In addition, a path prediction algorithm [33] is also used to estimate and judge the current vehicles locations

B. Used Notations

The following table summarize the main used notations and there meanings:

TABLE I: Used notations.

Notation	Meaning
X	Integer Value
$k = T_t(x)$	Public key
PW	Password
ID_i	Identifier of the node 'i'
H()	Hash function
$Tr(i,j)$	Global Inter-vehicle trust
$DirectT(i,j)$	Inter-vehicle direct trust
$IndirectT(i,j)$	Inter-vehicle indirect trust
$RR(RSU,j)$	RoadSide Unit recommendation
$TAD(j))$	Trusted Authority's Decision

IV. TACASHI'S TRUST ESTABLISHMENT

As mentioned in the previous sections, our proposal involves drivers honesty (see figure 5), vehicles honesty (see figure 6), and vehicles-location related honesty (see figure 7). before detailing in the following sections how these factors are computed, the next section presents the proposed in-vehicle inter-device secure communication process.

[2]The SmartCarPhone project, http://www.grc.upv.es/SmartCarPhone/

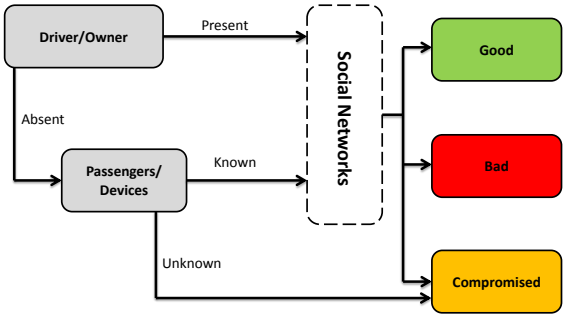

Fig. 5: Driver and passengers honesty factor.

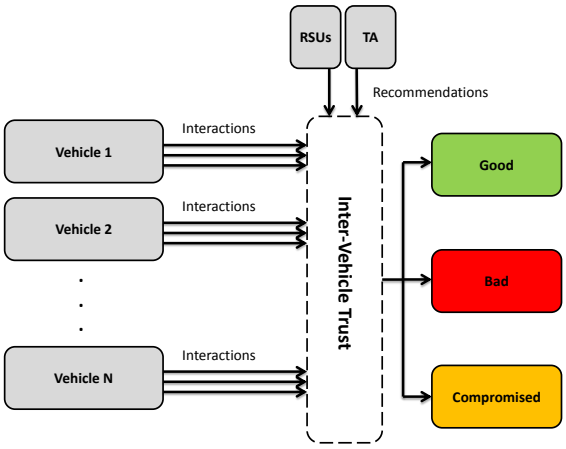

Fig. 6: Vehicles honesty factor.

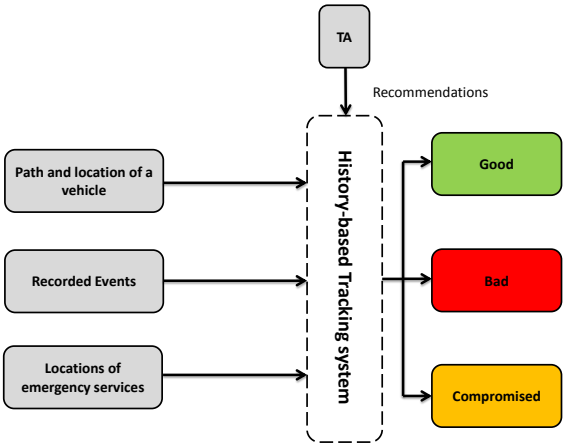

Fig. 7: Location-related honesty factor.

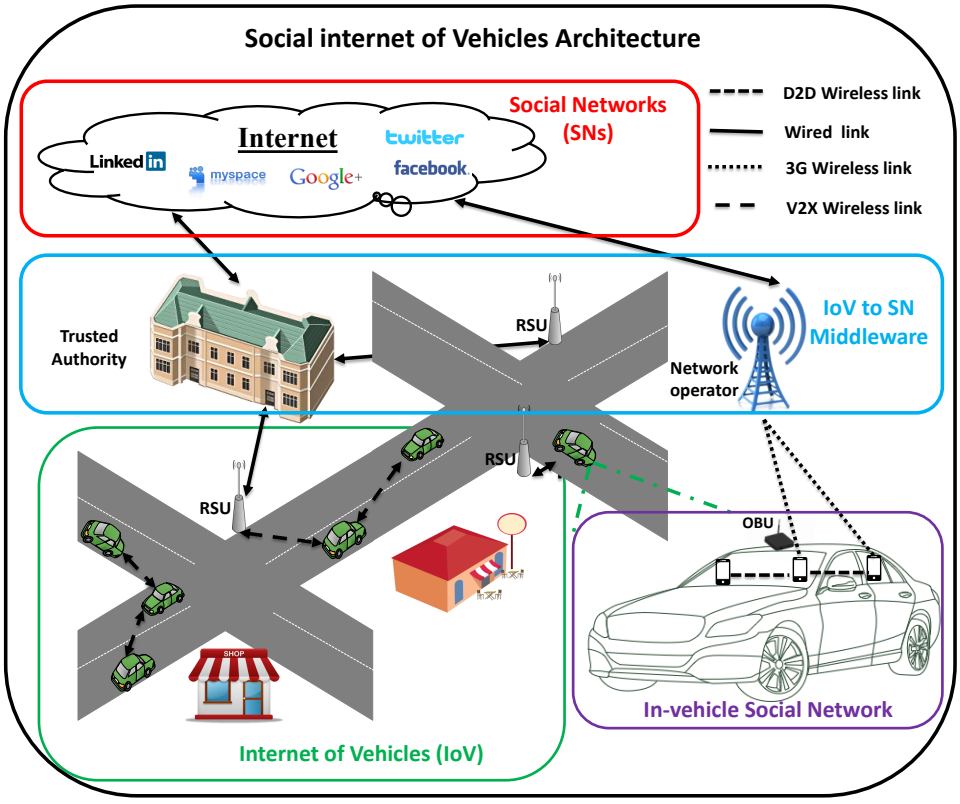

Fig. 4: Proposed Social Internet of Vehicles Architecture.

A. *In-vehicle inter-devices authentication process*

In order to enable OSN-based trust while preserving drivers/owners privacy, department of motor vehicles (DMV) initializes the OBU by performing a number of operations. First the driver enters its anonymized OSN account and DMV registers it against the user. DMV also issues a number of pseudonyms $\{ID_1^a, ID_2^a, ..., ID_n^a\}$ to a user 'a'.

In-vehicle device/passengers in TAKASHI are required to pass the authentication process before accessing the different network operations. If these devices fait to be authenticated they are directly classified as compromised devices as shown in figure 5.

We assume that all the devices in a network have identity(ID_i) and get the secure token from Trusted Authority (TA), this token is assumed to be received through a secure channel.

All the nodes compute the public key $(x, Tk(x))$ and private key k using Chaotic Maps based Chebyshev polynomials which are known to be less energy consuming than RSA and ECC [34] .

Consider the communication between devices A and B with their identities ID_a and ID_b and their public and private key pairs are $\{(x, Tk_a(x)), k_a\}$ and $\{(x, Tk_b(x)), k_b\}$ respectively.

Let node A wants to securely communicate with node B, it initiates the authentication request as follows:

1) The device 'A' selects a prime number 'p' and compute the value of $T_p(x)$.
2) The node 'A' sends the message $ma = \{H_a, C_a\}$ to node 'B'.
3) After getting the message $ma = \{H_a, C_a\}$ from node 'A', 'B' decrypts C_a with the key $k = T_t(x)$ received from TTP, and compares the value of 'PW' from decrypted message with its obtained 'PW' value from TTP. If there is a match, then node 'B' concludes that 'A' is an authenticated node.
4) Afterwards, it checks the message integrity by computing the hash value and compares it with H_a, if there is a match, then 'B' concludes that the message is not altered during the communication.
5) Now node 'B' selects the big prime value 'b' and compute the values of $T_b(x)$, K_s, H_b, and C_b.
6) The node 'B' sends the message $mb = \{H_b, C_b, T_b(x)\}$ to node 'A'.
7) After getting the message $mb = \{H_b, C_b, T_b(x)\}$ from node 'B', 'A' computes the value of $K_s = T_{pb}(x) = T_p(T_b(x))$ by using $T_b(x)$ from message mb. Then Node 'A' decrypts C_b with the key K_s and compares the value of 'PW' from decrypted message with its obtained 'PW' value from TTP. If there is a match, then node 'A' concludes that 'B' is an authenticated node.
8) Afterwards, it checks the message integrity by computing the hash value and compares it with H_b, if there is a match, then 'B' concludes that the message is not altered during the communication.
9) Finally, both the nodes 'A' and 'B' agree on identical

session key K_s and further communication is encrypt and decrypt by session key K_s.

Detailed algorithm is shown figure 8.

B. Inter-vehicle trust

Inter-vehicle trust is composed of two main metrics which are the direct and indirect trusts.

The interaction-based trust ($DirectT(i,j)$) of the vehicle j evaluated by another vehicle i is the ratio of honest actions $\#H(i,j)$ to the total number of actions (both honest and dishonest $\#All(i,j)$). Therefore, the interaction-based trust is calculated in the following way:

$$DirectT(i,j) = \frac{\#H(i,j)}{\#All(i,j)} \cdot \Big[1 - \frac{1}{H(i,j)+1}\Big] \quad (1)$$

From equation 1, we can see that $1 - \frac{1}{H(i,j)+1}$ increases in respect of the increased number of honest actions, in such way that, several honest actions are needed to increase the interaction-based trust.

In our proposal, the inter-vehicle exchanged opinions (Indirect trust) are sent together with the unencrypted part of exchanged data messages. To favor the opinions sourced by vehicles considered as trusted, received recommendation (opinion) sourced by a vehicle k concerning the behavior of the vehicle j ($IndirectT_k(i,j)$) are combined with respect to the honesty level of the recommender k as described in equation 2:

$$IndirectT_k(i,j) = \big[DirectT(i,k) \cdot Recom(k,j)\big]^{\frac{1}{2}} \quad (2)$$

Then, the different vehicles' recommendation about vehicle j are combined together to find the global vehicles' recommendation value for that vehicle $RV(i,j)$ following equation 3:

$$IndirectT(i,j) = \Big[\prod_{|Recom|}^{k} IndirectT_k(i,j)\Big]^{\frac{1}{|Recom|}} \quad (3)$$

C. RoadSide Units Trust

Simultaneously with the different inter-vehicle interaction, whenever a vehicle joins the communication range of an RSU, it sends its different neighbors overall trust to this roadside unit. Afterwards, the RSU combines all vehicles reports to build a quasi global evaluation of the behavior of vehicles moving around.

Following Equation 4, the roadside units computes its opinion regarding any vehicle j through the combination of the reports delivered by the other vehicles.

$$RR(RSU,j) = \Big[\prod_{n}^{i} Tr(i,j)\Big]^{\frac{1}{n}} \quad (4)$$

In this equation, n represents the number of vehicles having previously evaluated the vehicle j

Algorithm 1 Location related Trust Classification

```
if Similarity(Predicted_Position(HistPath, Location, Time, ID), Current_Location(ID)) ≈ 1 then
    Location_Trust(ID)← Good;
else
    if Similarity(Position(Emergency_Services), Current_Location(ID)) ≈ 1 then
        Location_Trust(ID)← Compromised;
    else
        if Similarity(Position(Registered_Events), Current_Location(ID)) ≈ 1 then
            Location_Trust(ID)← Compromised;
        else
            Location_Trust(ID)← Bad;
        end if
    end if
end if
```

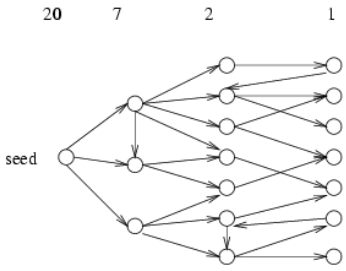

Fig. 9: Capacity assignment example.

D. Location related Trust

E. Social Networks trust using Advogato trust metric identifying trustable people

Various networking social aspects have been studied by an online free software developers community called Advogato. This community launched in 1999, has adopted a group-trust metric trying to determine the largest set of honest peers while minimizing the influence of unreliable dishonest ones [17]. Advogato uses a social graph to represent the network different peers and relations. Each peer in the graph is a user's account. Whereas, a directed edge represents a relation (also called 'certification').

The 'Advogato' trust metric stands on the network flow. it first assigns a 'capacity' C_i to every peer i, which represents a nonincreasing function of the distance separating the peer i and the seed, as returned by the the considered searching (breath-first algorithm). For instance, 'advogato.org' assigns a '800' capacity for the seed, then 200 for the following two levels, 50 for peers belonging to the third level, and so on (see figure 9).

Each node A is then divided into two sides, A- and A+, with a *capacity*-1 edge from A to the sink, and a capacity of(C_i-1) edge from A- to A+. Finally, the certification of A to B becomes an infinite-capacity edge from A+ to B- (see figure 10).

To find the maximum flow [35], Advogato is based on

Device A	Device B

Select a prime number 'p'
Compute the: T_p (x)
H_a = H (ID_a ||ID_b ||T_p(x)||PW)
C_a = Ek {T_p(x)|| PW}

$m_a = \{H_a, C_a\}$ →

$D_k(C_a) = \{T_p(x)||\ PW\}$
Compare the PWvalue,
If there is a match Then A is authenticated user
Compute Hash function
H(ID_a ||ID_b ||T_p(x)||PW) and
Compare it with H_a If there is a match Then
Message not tampered
Select a prime number 'b'
Compute the: T_p(x), $K_s = (T_p(x))$
H_b = H(ID_a ||ID_b ||T_b (x)||PW)
C_b = E{T_b (x)|| PW}

← $M_b = \{H_b, C_b, T_b(x)\}$

Compute the: $K_s = (T_b(x))$
$D_{ks}(C_b) = \{T_b(x)||PW\}$
Compare the PW value
If there is a match Then B is authenticated user
Compute Hash function
H(ID_b ||ID_a ||T_b (x)||PW), and
Compare it with Ha If there is a match Then
Message is not tampered

Agree on Session Key Ks = $(T_b(x)) = T_b(T_p(x)) = T_{pb}(x)$ ↔

Fig. 8: In-vehicle Device-to-device secure communication.

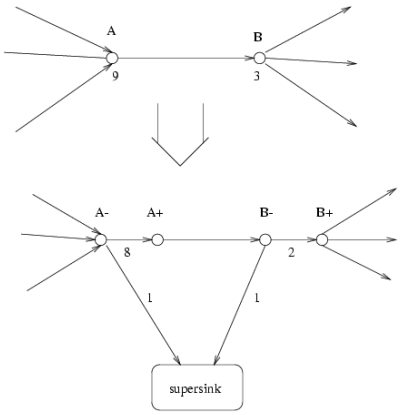

Fig. 10: Conversion into a single source, single sink.

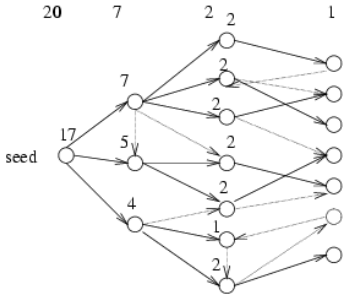

Fig. 11: Network flow computation.

the Ford-Fulkerson algorithm (see figure 11). Since Ford-Fulkerson selects the shortest increasing path from the current node to the seed, any node having a flow from x- to x+ possesses also a flow from x- to the sink. Ford-Fulkerson takes $O(|f+||E|)$, where f is the maximum flow. In this graph, $f+$ is the number of accepted peers.

Concerning the trusted accounts identification, an adversary model should be defined first. Then, the minimum cut is created to distinguish between trusted, doubted, and compromised accounts, as shown in figure 12. The graph's minimum cut is the one (a partition of the nodes of a graph into two or more - k-cut - disjoint subsets that are joined by at least one edge) that is minimal in some sense (trust value in our case) [36], [37].

We note that the Advogato trust metric has a wide range of applicability, meaning that edges and connections can be defined in a different ways, including for instance communities, friendship, shared posts, comments, or likes.

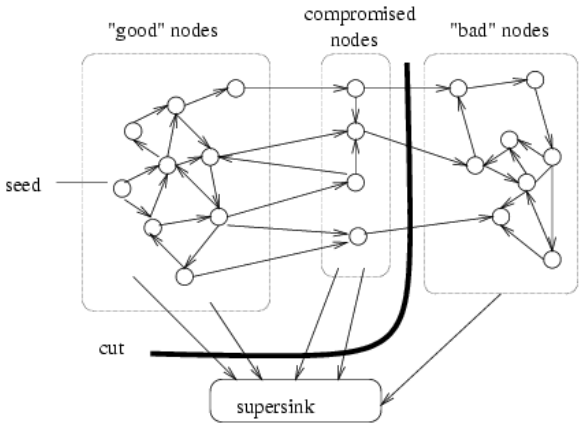

Fig. 12: Nodes classification.

V. TACASHI's Dishonesty Detection Process

In addition to the direct and recommendation-based trust, TAKASHI involves also the driver's honesty factor based on their OSN profiles, this information is received through the trusted middelware which is for our case the trusted authority, deployed RSUs, or even network operators. Furthermore, vehicles-location-related honesty is also taken into account in the overall trust evaluation.

If a vehicle has already demonstrated its honesty, and thereby benefits from an high trust value, there is no need to take the driver's honesty factor into account, and vice versa. Thus, nodes requiring the human honesty factor as complementary data should be only those nodes whose behaviour is unclear/compromised.

Depending on the online social networks trust computed through the Advogato trust metric, the trusted authority matches, for each vehicle identity, an honesty factor called 'Honesty Human Factor' (HHF), which refers to the Human Trust Factor of the current driver, a factor that varies within the range of $[-0.5, -0.2]$ for the drivers judged bad, $[-0.2, 0]$ for the drivers judged compromised, and $[0, +0, 2]$ for the drivers judged good.

In addition, using a path prediction algorithm [33] and based of algorithm 1 the Location-Related Honesty factor (LRH) is also considered. Similar to the HHF, LRH varies in the range of $[-0.5, -0.2]$ for the positions judged bad, $[-0.2, 0]$ for the positions compromised, and $[0, +0, 2]$ for the positions judged good.

Once the soliciting vehicles receive the HHF and LRH for neighbors they have concerns about, the trust computation will follow algorithm 2:

Where $Tr(i,j)$ is the global inter-vehicle trust, $RV(i,j)$ is the recommendation coming from a nearby vehicle, $RR(RSU,j)$ is the recommendation requested and received from a nearby RoadSide Unit, and finally, $RT(TA,j)$ is the trusted authority evaluation about the vehicle j's honesty.

In this equation, we test the trust evaluation $Tr(i,j)$ after every update to keep it within the range [0, 1].

Using this strategy, the number of dubious nodes will be reduced. Thus, a decision about vehicles trustiness can be made. This latter is made using the different vehicles reports

Algorithm 2 The overall inter-vehicle trust computation

if There is RSU Or traffic is delay-sensitive **then**
  $Tr(i,j) = \left[DirectT(i,j) \cdot RV(i,j)\right]^{\frac{1}{2}}$;
else
  if There is an RSU And the exchanged traffic is partially delay-sensitive **then**
    $Tr(i,j) = \left[DirectT(i,j) \cdot RR(j)\right]^{\frac{1}{2}}$;
  else
    if There is an RSU And the exchanged traffic delay-tolerant **then**
      $Tr(i,j) = TAD(j)$;
    else
      if j is a dubious node $(i.e,\ 0.4 \geq Tr(i,j) \geq 0.6)$ **then**
        $Tr(i,j) = Tr(i,j) + HHF(j) + LRH(j)$;
      end if
    end if
  end if
end if

to generate a blacklist of the detected misbehaving vehicles following equation 5.

$$RSUBlacklist = \forall j, \quad \frac{Card(j/\ \ Tr(i,j) \leq 0.5)}{Card(RC(j))} \geq DThreshold \tag{5}$$

Where $DThreshold$ represent the threshold besides which a vehicle is blacklisted. This threshold is compared with the ratio of negative reports about a vehicle j to the total number of reports.

The Trusted Authority's recommendations are in fact decisions that must be followed by the different sub-levels (RSUs and vehicles). It makes a decision $TAD(j)$ about a vehicle j. TA decisions are used only for non-sensitive delay applications as they involve all the lower levels evaluations which implies additional computation delays. Therefore, the trusted authority decision is computed following equation 6.

$$TAD(j) = \left[\prod_{n}^{i} RR(RSU_i, j)\right]^{\frac{1}{n}} \tag{6}$$

In this equation, n represents the number of RSUs having previously evaluated the vehicle j

VI. Performance Evaluation

Our proposal is implemented in NS-2.35 simulator. In addition, we used the same dataset as in [38]. This dataset called Epinions [39] has 131,828 nodes (users) and 841,372 edges (honest or malicious), we also consider that 30% of the edges represent a distrust relationship, and they are towards the 10% and 20% vehicles considered as dishonest. Hence, we considered in every case 10% of false evaluation (false positives). We selected the first 400 nodes that have more than 40 out-neighbors and we randomly matched their identities to 400 vehicle identities. Thus, every vehicle driver is represented

Fig. 13: Simulated city roadmap.

by a node within the used dataset. Furthermore, in every vehicle we have four devices one of them is assumed unknown.

For VANET settings, the traffic is generated using the Citymob mobility model [40]. In our case we used a $4km^2$ map of Laghouat city in Algeria (see figure 13) the generated vehicles path of 80% of the vehicles to enable the paths prediction. For the 20 % remaining vehicles, half of them are moving towards predefined positions called Emergency Location and Event Location (i.e, hospital, Soccer stadium ...etc.), and the other half are assumed to move to unpredictable positions. The scenario has 4 randomly deployed RSUs. We run our simulation 15 times to reach the 95% confidence.

The rest simulation parameters are summarized in Table II:

TABLE II: Simulation parameters.

Parameters	Value
Experiment duration (s)	1000
Communication range (m)	300
Vehicles speed (km/h)	[0,80]
Dishonesty ratio (%)	{10, 20}
Number of packet sources	10
Packet size (bytes)	256
Packet rate per second	4

First of all, we study the distribution of inter-vehicle trust with and without the driver honesty consideration. Afterwards, we compare the obtained dishonesty detection ratios compared to RTM [31] and AD-IoV [29]. Finally, we analyze the generated error ratios with and without the use of our proposed OSN-aided trust architecture.

A. Distribution of inter-vehicle trust

Making the right detection decision is an important task in any security system. Thus, the best case for these systems is to clearly identify whether the peers are honest or dishonest with a reduced margin of error. Figure 14 represents the different vehicles trust in respect of time when we do not rely on the human factor computed from OSNs. It depicts that, although the majority of peers have increased their trust (i.e, good behavior), many other peers still have a trust evaluation $0.4 \leq Tr(i,j) \geq 0.6$ which represents an unclear behavior leading mostly to wrong decisions.

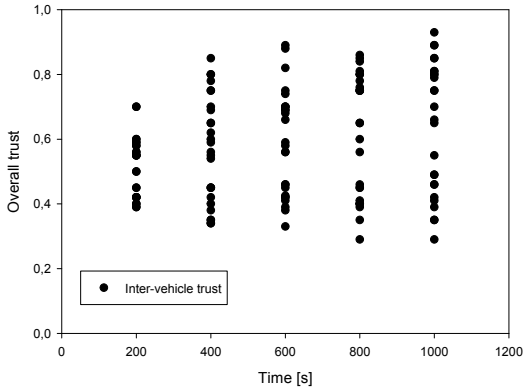

Fig. 14: Distribution of inter-vehicle trust without the human factor consideration.

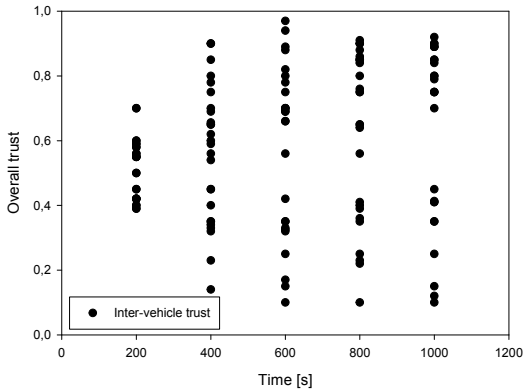

Fig. 15: Distribution of inter-vehicle trust when considering the human factor.

However, when the human weighting factor is used, we notice that almost all vehicles have either a clear positive ($Tr(i,j) \geq 0.6$) or negative trust ($Tr(i,j) \leq 0.4$), making the detection decision easy to make (see figure 15).

B. Detection performance

For the detection performance we also studied both cases with and without human factor consideration. Figure 16 representing the obtained detection ratio without using HHF for respectively 10% ad 20% of dishonest vehicles in respect of time. It shows that even though the average detection ratio exceeds the 90% for 10% malicious, the confidence interval is quite large reaching the 5% at the end of the various runs. This is mainly because of the doubtful behavior of some peers that must be weighted to either good or bad behavior. On the other hand, when the human factor is considered (see figure 17), the detection ratio reaches up to 96% for 10% dishonest vehicles and 93% for 20% case, with clearly more reduced confidence intervals.

Confirming the previous results, generated false positive in respect of time is optimized by more than 3% with more

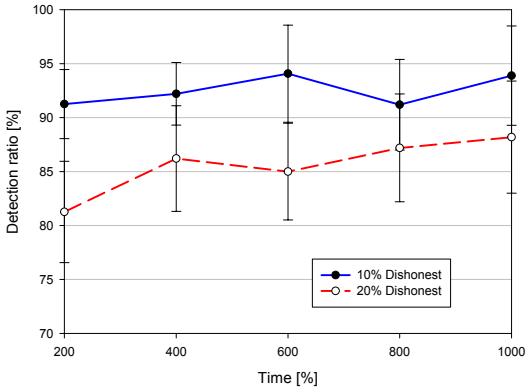

Fig. 16: Detection performance without the human factor consideration.

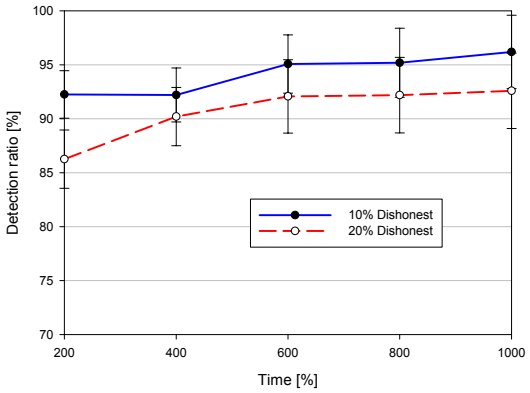

Fig. 17: Detection performance when considering the human factor.

reduced confidence intervals compared to the case with no human factor consideration (see figure18)

VII. Conclusion

In most of the existing works, vehicular social networks (VSNs) are considered as a set of vehicles moving with the same mobility patterns, going towards the same destination, or sharing specific applications. In this paper, we studied another dimension of VSNs by combining both online social networks and vehicular networks. Based on Advogato trust metric, we proposed to match the drivers honesty as a weighting factor to enhance the inter-vehicle trust establishment. Obtained results show that the human factor consideration have clearly enhanced the detection ratios of dishonest vehicles while reducing the generated error ratio.

For the future work, we plan to use and compare other datasets with a higher number of nodes and edges. We plan also to propose a combined simulation platform for OSNs and VANETs instead of simulating them in different platforms. Some other adversary models and privacy issues are also among the planned tasks.

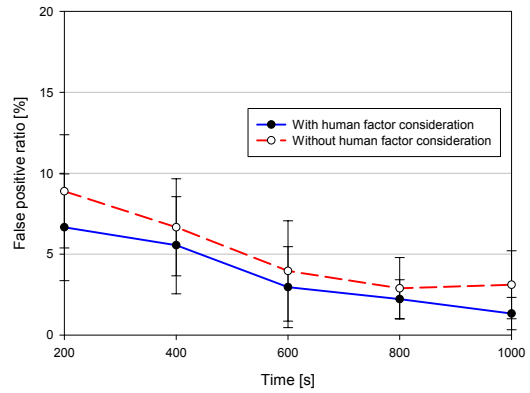

Fig. 18: Generated false positive.

References

[1] Y. Wang and F. Li, "Vehicular ad hoc networks," in *Guide to wireless ad hoc networks*. Springer, 2009, pp. 503–525.

[2] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in internet of vehicles: A review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339–2352, 2015.

[3] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Internet of Things (WF-IoT), 2014 IEEE World Forum on*. IEEE, 2014, pp. 241–246.

[4] A. M. Vegni and V. Loscri, "A survey on vehicular social networks," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2397–2419, 2015.

[5] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[6] K. M. Alam, M. Saini, and A. El Saddik, "Toward social internet of vehicles: Concept, architecture, and applications," *IEEE access*, vol. 3, pp. 343–357, 2015.

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

[8] S. Mumtaz, K. M. S. Huq, M. I. Ashraf, J. Rodriguez, V. Monteiro, and C. Politis, "Cognitive vehicular communication for 5g," *IEEE Communications Magazine*, vol. 53, no. 7, pp. 109–117, 2015.

[9] S. Patra, J. H. Arnanz, C. T. Calafate, J.-C. Cano, and P. Manzoni, "Eyes: A novel overtaking assistance system for vehicular networks," in *International Conference on Ad-Hoc Networks and Wireless*. Springer, 2015, pp. 375–389.

[10] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39–68, 2007.

[11] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, Y. Xiong, and X. Cui, "Attacks and countermeasures in the internet of vehicles," *Annals of Telecommunications*, vol. 72, no. 5-6, pp. 283–295, 2017.

[12] S. S. Manvi and S. Tangade, "A survey on authentication schemes in vanets for secured communication," *Vehicular Communications*, 2017.

[13] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[14] T. Gazdar, A. Rachedi, A. Benslimane, and A. Belghith, "A distributed advanced analytical trust model for vanets," in *Global Communications Conference (GLOBECOM), 2012 IEEE*. IEEE, 2012, pp. 201–206.

[15] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "Tfdd: A trust-based framework for reliable data delivery and dos defense in vanets," *Vehicular Communications*, 2016.

[16] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks," *IEEE transactions on vehicular technology*, vol. 64, no. 8, pp. 3657–3674, 2015.

[17] R. Levien and A. Aiken, "Attack-resistant trust metrics for public key certification." in *Usenix Security*, 1998.

[18] F. Xia, L. Liu, J. Li, J. Ma, and A. V. Vasilakos, "Socially aware networking: A survey," *IEEE Systems Journal*, vol. 9, no. 3, pp. 904–921, 2015.

[19] T. DuBois, J. Golbeck, and A. Srinivasan, "Predicting trust and distrust in social networks," in *Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on*. IEEE, 2011, pp. 418–424.

[20] Y. A. Kim and M. A. Ahmad, "Trust, distrust and lack of confidence of users in online social media-sharing communities," *Knowledge-Based Systems*, vol. 37, pp. 438–450, 2013.

[21] S. Brin and L. Page, "Reprint of: The anatomy of a large-scale hypertextual web search engine," *Computer networks*, vol. 56, no. 18, pp. 3825–3833, 2012.

[22] J. Zhang, "A survey on trust management for vanets," in *Advanced information networking and applications (AINA), 2011 IEEE international conference on*. IEEE, 2011, pp. 105–112.

[23] N. Yang, "A similarity based trust and reputation management framework for vanets," *International Journal of Future Generation Communication and Networking*, vol. 6, no. 2, pp. 25–34, 2013.

[24] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "Trust and exclusion in vehicular ad hoc networks: an economic incentive model based approach," in *Computing, Communications and IT Applications Conference (ComComAp), 2013*. IEEE, 2013, pp. 13–18.

[25] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *International Conference on Network and System Security*. Springer, 2013, pp. 94–108.

[26] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "Tfdd: A trust-based framework for reliable data delivery and dos defense in vanets," *Vehicular Communications*, vol. 9, pp. 254–267, 2017.

[27] C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni, "T-vnets: A novel trust architecture for vehicular networks using the standardized messaging services of etsi its," *Computer Communications*, vol. 93, pp. 68–83, 2016.

[28] J. Contreras, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of vehicles: Architecture, protocols, and security," *IEEE Internet of Things Journal*, 2017.

[29] S. Yang, Z. Liu, J. Li, S. Wang, and F. Yang, "Anomaly detection for internet of vehicles: A trust management scheme with affinity propagation," *Mobile Information Systems*, vol. 2016, 2016.

[30] M. Hossain, R. Hasan, and S. Zawoad, "Trust-iov: A trustworthy forensic investigation framework for the internet of vehicles (iov)," in *Internet of Things (ICIOT), 2017 IEEE International Congress on*. IEEE, 2017, pp. 25–32.

[31] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Trust on the ratee: A trust management system for social internet of vehicles," *Wireless Communications and Mobile Computing*, vol. 2017, 2017.

[32] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: a survey on architecture, challenges, and solutions," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2377–2396, 2015.

[33] P. Lytrivis, G. Thomaidis, M. Tsogas, and A. Amditis, "An advanced cooperative path prediction algorithm for safety applications in vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 669–679, 2011.

[34] P. Bergamo, P. D'Arco, A. De Santis, and L. Kocarev, "Security of public-key cryptosystems based on chebyshev polynomials," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 52, no. 7, pp. 1382–1393, 2005.

[35] L. R. Ford and D. R. Fulkerson, "Maximal flow through a network," *Canadian journal of Mathematics*, vol. 8, no. 3, pp. 399–404, 1956.

[36] P. An, P. Keck, and T. Kim, "Min-cut algorithms."

[37] M. Stoer and F. Wagner, "A simple min-cut algorithm," *Journal of the ACM (JACM)*, vol. 44, no. 4, pp. 585–591, 1997.

[38] S. Al-Oufi, H.-N. Kim, and A. El Saddik, "A group trust metric for identifying people of trust in online social networks," *Expert Systems with Applications*, vol. 39, no. 18, pp. 13 173–13 181, 2012.

[39] J. Leskovec, D. Huttenlocher, and J. Kleinberg, "Signed networks in social media," in *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 2010, pp. 1361–1370.

[40] F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Citymob: a mobility model pattern generator for vanets," in *Communications Workshops, 2008. ICC Workshops' 08. IEEE International Conference on*. IEEE, 2008, pp. 370–374.