Document downloaded from:

http://hdl.handle.net/10251/157307

This paper must be cited as:

Kerrache, CA.; Lagraa, N.; Hussain, R.; Ahmed, SH.; Benslimane, A.; Tavares De Araujo Cesariny Calafate, CM.; Cano, J.... (2019). TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles. IEEE Internet of Things. 6(4):5870-5877. https://doi.org/10.1109/JIOT.2018.2880332

The final publication is available at

https://doi.org/10.1109/JIOT.2018.2880332

Copyright Institute of Electrical and Electronics Engineers

Additional Information

TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles

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

***Abstract*—The Internet of Vehicles (IoV) has emerged as a new spin-off research theme from traditional vehicular ad hoc networks. It employs vehicular nodes connected to other smart objects equipped with a powerful multisensor platform, communication technologies, and IP-based connectivity to the Internet, thereby creating a possible social network called Social IoV (SIoV). Ensuring the required trustiness among communicating entities is an important task in such heterogeneous networks, especially for safety-related applications. Thus, in addition to securing intervehicle communication, the driver/passengers honesty factor must also be considered, since they could tamper the system in order to provoke unwanted situations. To bridge the gaps between these two paradigms, we envision to connect SIoV and online social networks (OSNs) for the purpose of estimating the drivers and passengers honesty based on their OSN profiles. Furthermore, we compare the current location of the vehicles with their estimated path based on their historical mobility profile. We combine SIoV, path-based and OSN-based trusts to compute the overall trust for different vehicles and their current users. As a result, we propose a trust-aware communication architecture for social IoV (TACASHI). TACASHI offers a trust-aware social in-vehicle and intervehicle communication architecture for SIoV considering also the drivers honesty factor based on OSN. Extensive simulation results evidence the efficiency of our proposal, ensuring high detection ratios >87% and high accuracy with reduced error ratios, clearly outperforming previous proposals, known as RTM and AD-IoV.**

***Index Terms*—Human factor, Social Internet of Vehicles (SIoV), trust, vehicular ad hoc network (VANET).**

I. Introduction

Many applications have been realized through vehicular networks as a result of communication among vehicles and/or the infrastructure [1]. These applications are abstractly classified into safety and nonsafety related applications. The former class of applications exhibit stringent requirements, such as delay-critical, security-critical, trust-critical, and decision-critical features, whereas the latter class of applications have relatively less stringent requirements. Nevertheless, many of these applications represent a decision-aided system where the final decision (usually taken by the human drivers) have a direct effect on the outcome of the decision. Therefore, the trustworthiness of the information and the source of information is of prime importance.

In Internet of Vehicles (IoV) paradigm, each vehicle is considered as a smart object equipped with a powerful multisensor platform, communications technologies, computation units, IP-based connectivity to the Internet, and to other vehicles either directly or indirectly. In addition, a vehicle in IoV is envisioned with a multicommunication model, enabling the interactions among intravehicle components, intervehicles, vehicle-to-infrastructure, and vehicles-to-people. IoV also enables the acquisition 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 [2].

To this end, the communication of vehicles with different entities in IoV exhibit social features at par with the traditional social networks where the nodes share information. More precisely, Social IoV (SIoV) are a breed of socially aware ephemeral networks [3], where vehicular nodes share/exchange information with different entities and thusforth comparable with the traditional social networks. On the other hand, with the emergence of 5G technology, almost all Internet services can be accessed anytime and anywhere [4]. In addition, vehicles' mobility patterns can be easily estimated through its history profiles and the drivers' social interactions and hobbies. Hence, the SIoV system can trigger a possible event, which would advocate for verification of the situation, resulting in stolen vehicle alert an alert or even, text the vehicle's owner. It is indeed possible that there could be false alarms; however, more insights are needed to this issue.

To fill the gaps, 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 considering the human and location-related honesty (LRH). We leverage the group-trust metric adopted by Advogato,[1]

C. A. Kerrache is with the Department of Mathematics and Computer Science, University of Ghardaia, Ghardaïa 47000, Algeria (e-mail: ch.kerrache@lagh-univ.dz).

N. Lagraa is with the University of Laghouat, Laghouat 03000, Algeria (e-mail: n.lagraa@lagh-univ.dz).

R. Hussain is with the Institute of Information Systems, Innopolis University, 420500 Innopolis, Russia (e-mail: r.hussain@innopolis.ru).

S. H. Ahmed is with the Department of Computer Science, Georgia Southern University, Statesboro, GA 30460 USA (e-mail: sh.ahmed@ieee.org).

A. Benslimane is with the University of Avignon, 84911 Avignon, France (e-mail: abderrahim.benslimane@univ-avignon.fr).

C. T. Calafate and J.-C. Cano are with the Department of Computer Engineering, Universitat Politècnica de València, Valencia, Spain (e-mail: calafate@disca.upv.es; jucano@disca.upv.es).

A. M. Vegni is with the Department of Engineering, Roma Tre University, 00146 Rome, Italy (e-mail: annamaria.vegni@uniroma3.it).

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

attempting to determine the maximum set of trusted peers, while minimizing the influence of unreliable dishonest peers during communication [5]. Afterward, an honesty-related classification (i.e., good, bad, or compromised) is associated to every node (driver/passenger) and vehicle location depending on the Advogato classification of this node (i.e., either trusted or distrusted) and the location tracking system, respectively. In addition, in-vehicle interdevice communications are secured using a lightweight technique based on Chaotic Maps.

Furthermore, the intervehicle trust is also estimated, combined with the discrete recommendations from RSUs and trusted authorities (TAs). Finally, the Advogato results are used to probabilistically identify honest and dishonest drivers/passengers. Using this strategy, the aim is not just to reduce both the detection error ratios and also the ratio of doubtful nodes that the intervehicle trust could not classify them to either trusted or distrusted peers but also to prevent unwanted situations, such as stolen vehicles thanks to the LRH estimation.

To summarize, the contributions of this paper are as follows.

1) We propose a trust-aware communication architecture for social IoV (TACASHI), which offers a trust-aware social in-vehicle and intervehicle communication architecture for SIoVs.
2) Secure in-vehicle communications are guaranteed through Chaotic Maps.
3) Drivers' honesty consideration using their OSN profiles reached through a trusted middleware.
4) Vehicles movement-related honesty estimation through the use of their historical mobility patterns and a path prediction algorithm.

The remainder of this paper is organized as follows. In Section II, we present some background in vehicular ad hoc network (VANET), IoV, OSNs, and trust establishment in both kinds of networks. Afterward, in Section III, we present an overview of our proposal, followed by its details in Section IV. TACASHI's dishonesty detection process is then discussed in Section V. Section VI presents our simulation environment, followed by the discussion of the results obtained. Finally, the conclusions are drawn at the end of this paper.

II. State-of-the-Art

Trust establishment in vehicular networks is essential for the realization of efficient secure applications. Various solutions have adopted trust modeling to enhance the intervehicle communications for VANETs, IoV, and SIoV. In this section, we provide an overview of the main features of socially aware networking, as well as the existing trust-based solutions in these domains.

A. Social Trust and Socially Aware Networking

The proliferation of hand-held devices demands mobile carriers to provide instant connectivity. Moreover, the movements of the users are generally related to their social behaviors and relationships, and the mobility patterns of mobile devices carried by these users are strongly coupled with their movements. Thus, mobile networks are nowadays more human-centric. As a result, a new field called socially aware networking has surfaced that takes the human behavior into account [6]. This new paradigm of social-awareness is applicable to many types of internode interaction-based networks, such as ad hoc networks and its different breeds.

B. Trust in OSNs

As aforementioned, trust establishment is primarily important for enhancing the security of different networks and many solutions used trust establishment mechanisms for OSNs [7], [8]. The general trust establishment solutions for OSNs are based on either Advogato trust metric [5] or PageRank-based solutions [9].

Generally, trust for OSNs can be classified using three complementary phases: 1) trust information collection; 2) trust evaluation; and 3) 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 forms and for different purposes.

C. Trust in VANETs and IoV

In the VANET context, trust management schemes are generally classified as entity-based, content-based, and hybrid models following the targeted adversary, which can be dishonest entities, malicious messages, or both [10]. Several works in the literature addressed entity-based trust models. Yang's [11] solution is based on revocation of the nodes that sent falsified or fake information using different techniques. Haddadou *et al.* [12] chose to associate a credit value to each neighbor vehicle that will increase or decrease depending on the messages credibility of the concerned neighbor's. Hence, this credit will be quickly decreased when replaying or injecting new (potentially false or malicious) messages.

For content-based trust management, Gurung *et al.* [13] adopted three metrics to classify the 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 exhibited by VANET nodes and the node sparsity. On the other hand, our previous hybrid models [14], [15] 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. Additionally, few solutions addressing trust issues in the IoV have also been recently published [16].

Hossain *et al.* [17] proposed a trust model for collecting evidence from IoV infrastructures, store them in vehicles tamper-proof devices, and then start intervehicle trust-based communication. The main limitation of such approach is that the behavior of vehicles may change. Thus, trust information values should remain static over time. In addition, authors did not evaluate the performance in a realistic environment implementing the different low-layer features of VANETs.

Unlike existing trust models, Gai *et al.* [18] proposed 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 to ensure the integrity and the undeniability of the trust information. However, besides the additional cost of the introduced server, this scheme may not be effective in rural scenarios or low-density scenarios. Furthermore, as like in other existing solutions, the human honesty factor is not considered.

D. Trust Computation in Vehicular Networks and OSNs

Due to the distributed and ephemeral nature of vehicular networks, every vehicle locally evaluates its neighbors' trust. This trust computation can be carried out 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 [19]. Whereas, trust in OSNs requires having a sink or a third trusted party who is responsible for evaluating the trust for 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 [20].

In the light of the existing works, there is a still a huge gap between the requirements of the trust-based communication in SIoV and the existing solutions. To fill the gaps, we propose a novel trust-based SIoV communication architecture (namely, TACASHI), which besides the intervehicle trust establishments evaluates also their drivers and movement honesty. Furthermore, TACASHI also offers a secure and lightweight in-vehicle communication strategy.

III. TACASHI Overview

Establishing SIoV trust with the incorporation of the human honesty factor should be achieved by relying on third TAs as intermediaries for this information, since these authorities are the only ones having the possibility to trace/track vehicles identities 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 TA. 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, 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 [21].

Fig. 1 represents an overview of our proposed SIoV architecture in which, besides passengers, vehicles, roadside units, and TAs, we also involve OSNs. The latter are accessed through a trusted middleware provided by the network operator, RSUs, or TA like the City Hall.

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

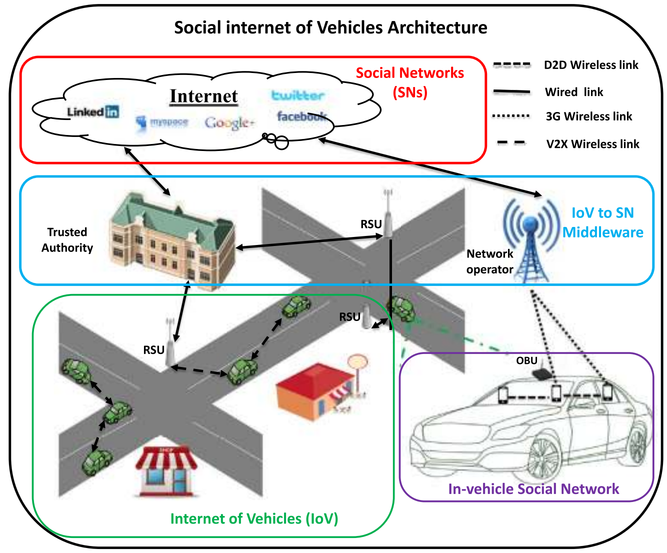

Fig. 1. Proposed SIoV architecture.

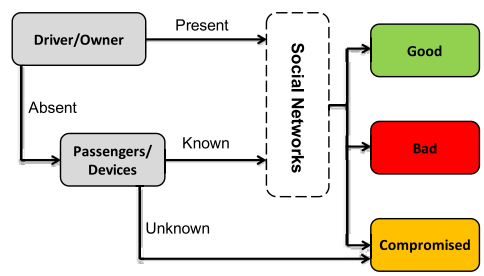

Fig. 2. Driver and passengers honesty factor.

TACASHI architecture involves five main actors: 1) the person registered as the vehicle owner; 2) the passengers within the vehicle represented by their connected devices; 3) the vehicles themselves; 4) road side units and TAs; and 5) the OSN accounts connected to the driver and passengers' devices. In addition, a path prediction algorithm [22] is also used to estimate and judge the current vehicle locations.

IV. TACASHI's Trust Establishment

As mentioned in the previous sections, our proposal involves drivers' honesty (see Fig. 2), vehicles' honesty (see Fig. 3), and vehicles' LRH (see Fig. 4). Before detailing how these factors are computed in the following sections, the next section presents the proposed in-vehicle interdevice secure communication process.

A. In-Vehicle Interdevices Authentication Process

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

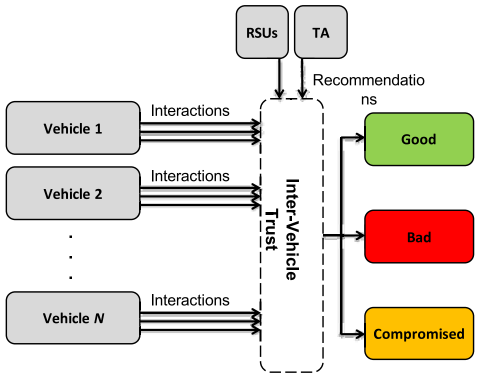

Fig. 3. Vehicles honesty factor.

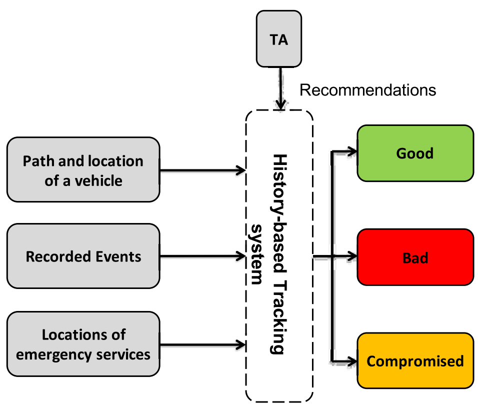

Fig. 4. LRH factor.

In-vehicle device/passengers in TACASHI are required to pass the authentication process before gaining access to the different network operations. If these devices fail to be authenticated, they are directly classified as compromised devices, as shown in Fig. 2.

We assume that all the devices in a network have an identity (ID_i), and get the secure token from the 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 on Chebyshev polynomials, which are known to be less energy consuming than RSA and ECC [23].

Consider the communication between devices A and B with their identities, i.e., 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.

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

1) Node A selects a prime number p and computes the value of $T_p(x)$.
2) 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 the 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) Afterward, 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 was not altered during the communication.
5) Now node B selects the big prime value b and computes the values of $T_b(x)$, K_s, H_b, and C_b.
6) 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 the 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) Afterward, 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 was not altered during the communication.
9) Finally, both the nodes A and B agree on an identical session key K_s and further communication is encrypted and decrypted by session key K_s.

B. *Intervehicle Trust*

Intervehicle trust is composed of two main metrics: 1) direct trust and 2) indirect trust.

The interaction-based trust, i.e., $(\mathrm{Direct}T(i, j))$, of the jth vehicle as evaluated by the ith vehicle, is the ratio of honest actions $\#H(i, j)$ to the total number of actions, i.e., both honest and dishonest $\#\mathrm{All}(i, j)$. It follows that the interaction-based trust is calculated as:

$$\mathrm{Direct}T(i, j) = \frac{\#H(i, j)}{\#\mathrm{All}(i, j)} \cdot \left[1 - \frac{1}{H(i, j) + 1}\right]. \qquad (1)$$

From (1), we can see that $1 - (1/[H(i, j) + 1])$ increases with respect to the increased number of honest actions in such a way that several honest actions are needed to increase the interaction-based trust.

In our proposal, the intervehicle exchanged opinions (i.e., Indirect trust) are sent together with the unencrypted part of exchanged data messages. To favor the opinions sourced by vehicles considered as trusted, the received recommendations (opinions) sourced by a vehicle k concerning the behavior of a vehicle j [i.e., $\mathrm{Indirect}T_k(i, j)$] are combined with respect to the honesty level of the recommender k, as follows:

$$\mathrm{Indirect}T_k(i, j) = \left[\mathrm{Direct}T(i, k) \cdot \mathrm{Recom}(k, j)\right]^{\frac{1}{2}}. \qquad (2)$$

Then, the different vehicles' recommendation about the jth vehicle are combined together to find the global vehicles' recommendation value for that vehicle $\mathrm{RV}(i, j)$, i.e.,

$$\mathrm{Indirect}T(i, j) = \left[\prod_{|\mathrm{Recom}|}^{k} \mathrm{Indirect}T_k(i, j)\right]^{\frac{1}{|\mathrm{Recom}|}}. \qquad (3)$$

C. *Road Side Units Trust*

Simultaneously with the different intervehicle interactions, whenever a vehicle joins the communication range of an RSU, it sends its different neighbors overall trust to the road side

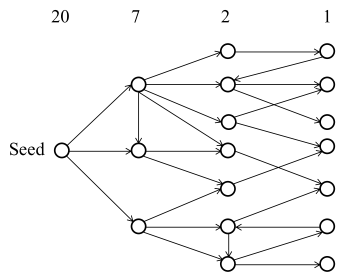

Fig. 5. Capacity assignment example.

unit. Afterward, the RSU combines all vehicles reports to build a quasi-global evaluation of the behavior of vehicles moving around.

Following (4), the roadside units compute their opinion regarding any vehicle j through the combination of the reports delivered by the other vehicles, i.e.,

$$\mathrm{RR}(\mathrm{RSU}, j) = \left[\prod_{n}^{i} \mathrm{Tr}(i, j)\right]^{\frac{1}{n}} \tag{4}$$

where n represents the number of vehicles having previously evaluated the jth vehicle.

D. Location-Related Trust

TACASHI classifies the LRH of a given vehicle through a similarity measurement between the current position and the estimated position, based on their historical mobility patterns [22]. Social events, such as soccer games, festivities, and emergency cases are also taken into account for the path estimation (see Fig. 4).

E. Social Networks Trust: Using the Advogato Trust Metric to Identify Trustable People

Various social networking 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 [5]. Advogato uses a social graph to represent the different peers and relations in the network. Each peer in the graph represents 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 considered searching (breath-first algorithm). For instance, "advogato.org" assigns a 20 capacity for the seed, then 7 for the following two levels, 2 for peers belonging to the third level, and so on (see Fig. 5).

Each node A is then divided into two sides, i.e., 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$+$, respectively. Finally, the certification of A to B becomes an infinite-capacity edge from A$+$ to B$-$ (see Fig. 6).

To find the maximum flow [24], Advogato is based on the Ford–Fulkerson algorithm (see Fig. 7). Since Ford–Fulkerson

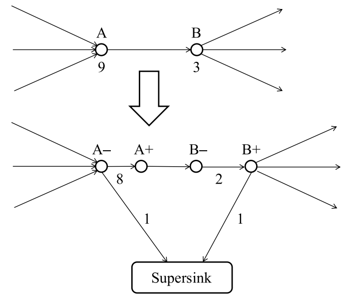

Fig. 6. Conversion into a single source, single sink.

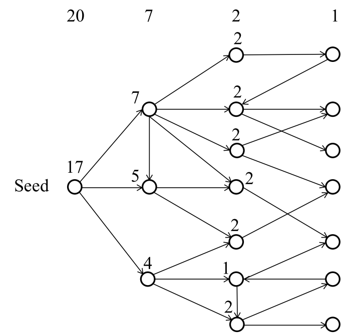

Fig. 7. Network flow computation.

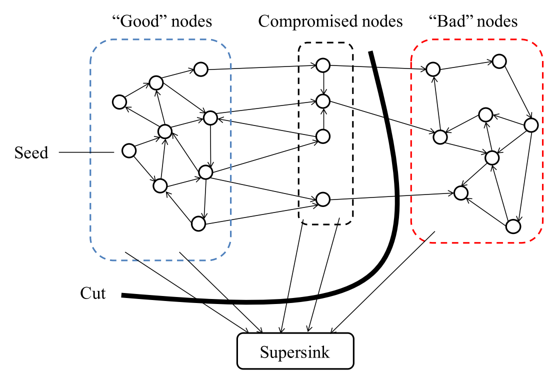

Fig. 8. Nodes classification.

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 Fig. 8. The graph's minimum cut (i.e., a partition of the nodes of a graph into two or more—k-cut—disjoint subsets that are joined by at least one edge) is the one that is minimal in some sense (trust value in our case). We note that the Advogato trust metric has a wide range of applications, meaning that edges and connections can be defined in different ways, including, for instance, communities, friendship, shared posts, comments, or likes.

Algorithm 1 Overall Intervehicle Trust Computation

if There is an 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 is 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

V. TACASHI'S DISHONESTY DETECTION PROCESS

In addition to the direct and recommendation-based trust, TACASHI involves also the driver's honesty factor based on their OSN profiles. This information is received through the trusted middleware, which for our case can be the TA, the deployed RSUs, or even network operators. Furthermore, the vehicles' LRH 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 behavior is unclear/compromised.

Depending on the OSNs, and having trust computed through the Advogato trust metric, the TA matches, for each vehicle identity, an honesty factor called honesty human factor (HHF), which refers to the human trust factor of the current driver. This factor varies within the range of $[-0.5, -0.2]$ for the drivers judged as bad, $[-0.2, 0]$ for the drivers judged as compromised, and $[0, +0, 2]$ for the drivers judged as good. Whereas, the overall trust is in the range of $[0, 1]$.

In addition, using a path prediction algorithm [22], the LRH factor is also considered.

Similarly to the HHF, the LRH varies in the range of $[-0.5, -0.2]$ for the positions judged as bad, $[-0.2, 0]$ for the positions that are compromised, and $[0, +0, 2]$ for the positions judged as good. Once the soliciting vehicles receive the HHF and LRH for neighbors they have concerns about, the trust computation will follow Algorithm 1. In this algorithm, $\mathrm{Tr}(i, j)$ is the global intervehicle trust, $\mathrm{RV}(i, j)$ is the recommendation coming from a nearby vehicle, $\mathrm{RR}(\mathrm{RSU}, j)$ is the recommendation requested and received from a nearby road side unit, and, finally, $\mathrm{RT}(TA, j)$ is the TA evaluation about the jth vehicle's honesty.

The trust evaluation $\mathrm{Tr}(i, j)$ is assessed 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 the vehicles' trustiness can be made. The latter is made by using the different vehicles reports to generate a blacklist of the detected misbehaving vehicles, i.e.,

$$\mathrm{RSUBlacklist} = \forall j \tag{5}$$

$$\frac{\mathrm{Card}(j/\ \ \mathrm{Tr}(i,j) \leq 0.5)}{\mathrm{Card}(\mathrm{RC}(j))} \geq D\mathrm{Threshold} \tag{6}$$

where DThreshold represents the threshold beyond which a vehicle is blacklisted. This threshold is compared with the ratio of negative reports about the jth vehicle to the total number of reports.

The TA's recommendations are in fact decisions that must be followed by the different sublevels (RSUs and vehicles). It makes a decision $\mathrm{TAD}(j)$ about the jth vehicle. TA decisions are used only for nondelay-sensitive applications, as they involve all the lower level evaluations, thus implying additional computation delays. Therefore, the TA decision is computed according to

$$\mathrm{TAD}(j) = \left[\prod_{n}^{i} \mathrm{RR}(\mathrm{RSU}_i, j)\right]^{\frac{1}{n}} \tag{7}$$

where n represents the number of RSUs having previously evaluated the jth vehicle.

VI. PERFORMANCE EVALUATION

Our proposal is implemented in the NS-2.35 simulator. In addition, we used the same dataset as in [25]. This dataset, called Epinions [26], 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 toward the 10% and 20% vehicles considered as dishonest. Hence, we considered in every case 10% of false evaluations (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 by a node within the used dataset. Furthermore, in every vehicle, we have four devices, being one of them assumed unknown.

For VANET settings, the traffic is generated using the Citymob mobility model [27]. In our case, we used a 4 km^2 map of Laghouat city in Algeria. The generated vehicles path of 80% of the vehicles to enable the paths prediction. For the 20% remaining vehicles, half of them are moving toward predefined positions called emergency location and event location (i.e., hospital, soccer stadium, and so on), and the other half are assumed to move to unpredictable positions. The scenario has four randomly deployed RSUs. We run our simulation for a duration of 1000 s 15 times to reach the 95% confidence level. In addition, the vehicles communication range is set 300 m and they are moving with a speed varying in the range of [0, 80] km/h. Finally, ten randomly chosen vehicles send four data packets of 256 bytes each every second.

In the following, we will compare the obtained dishonesty detection ratios to ones of RTM [18] and AD-IoV [28].

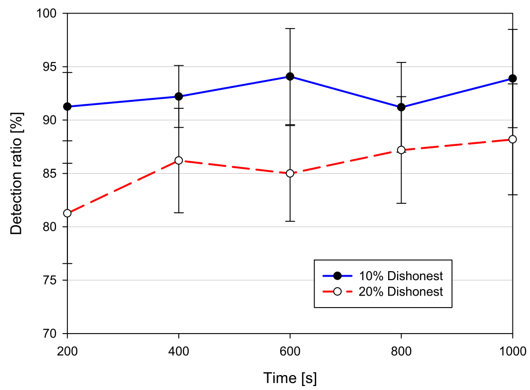

Fig. 9. Detection performance without the drivers honesty consideration.

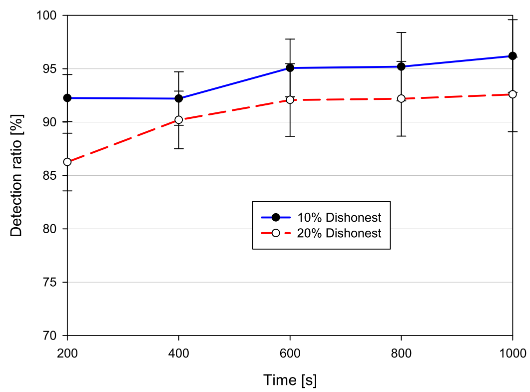

Fig. 10. Detection performance when considering the HF.

Afterward, we will analyze the generated error ratios with and without the use of our proposed OSN-aided trust architecture.

For the detection performance we also studied both cases, with and without human factor considerations. Fig. 9 represents the obtained detection ratio without using HHF for 10% and 20% of dishonest vehicles with respect to time, respectively. It shows that, although the average detection ratio exceeds the 90% for 10% of malicious nodes, 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 classified as behaving good or bad. On the other hand, when the human factor is considered (see Fig. 10), the detection ratio reaches up to 96% for 10% of dishonest vehicles, and 93% for the 20% case, with clearly more reduced confidence intervals.

Compared to the detection ratios achieved by RTM and AD-IoV, both TACASHI versions with (i.e., TACASHI+) and without (i.e., TACASHI-) driver's honesty consideration achieved higher detection ratios. Even more, with TACASHI+ the obtained detection ratios reach almost optimal performance, as depicted in Fig. 11. This is mainly due to the incorporation of OSN to enhance the trust establishment and, thus, reduce the detection error ratios.

Confirming the previous results, the number of generated false positives with respect of time is optimized by more than 3%, with more reduced confidence intervals compared to the case where the driver factor is not considered (see Fig. 12). However, the generated error ratio by both RTM and AD-IoV

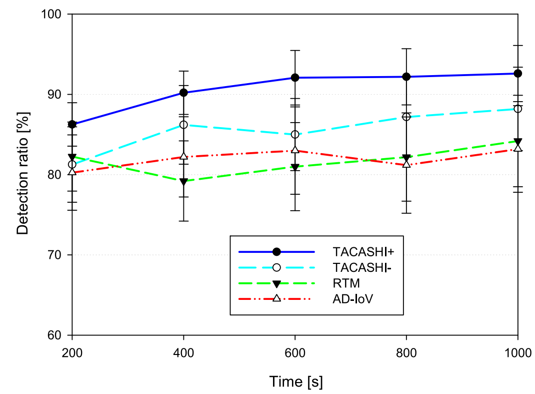

Fig. 11. Detection performance of TACASHI with and without considering the HF compared to RTM and AD-IoV.

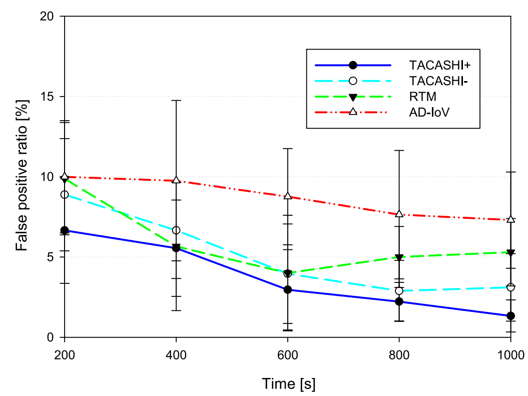

Fig. 12. Generated false positives by TACASHI with and without considering the HF compared to RTM and AD-IoV.

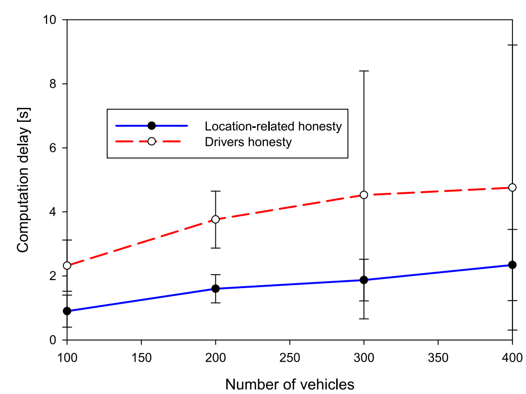

Fig. 13. TACASHI's introduced delay to compute HF and the LRH.

is quite high, reaching up to 10% for AD-IoV, which may cause some undesired situations.

Although the use of the OSNs and path prediction algorithms through the trusted middleware has enhanced the overall trust establishment, it is still prone to cause some additional delay which becomes unacceptable for safety applications. Fig. 13 presents the required computation delay of the drivers' honesty from OSNs and vehicles LRH through the trusted middleware. It shows that, on average, and based on the drivers honesty estimation, our proposal requires up to 5 s in the worst case. Indeed, this delay is not acceptable for IoV safety applications, but still it is considered reduced enough to prevent terrorist attacks or stolen vehicles. For the latter case, simulation results show that we can decide whether the current position of a given vehicle is normal or abnormal within less than 2 s in the worst case.

VII. Conclusion

IoV is composed of smart IP-based objects having connectivity to both the Internet and to other vehicles, forming a social network called SIoVs. Ensuring secure communication among these vehicles and their embedded devices is an essential requirement of SIoV, especially when these communications are related to safety applications. In this paper, we aimed at the trust-driven security mechanism for SIoV and proposed a novel trust-aware social in-vehicle and intervehicle communications architecture for SIoVs called TACASHI. In addition to the intervehicle trust establishment and lightweight secure in-vehicle communications, TACASHI also involves OSNs to estimate the honesty of vehicles' drivers. Furthermore, the historical mobility traces of the vehicles are stored and then used to estimate their future path, while also considering some exceptions, such as emergency situations and events. Simulation results demonstrate the performance of the proposed TACASHI at ensuring high misbehavior detection ratios clearly outperforms previous solutions known as RTM and AD-IoV.

As future work, we plan to add another social dimension to our architecture by also accounting for the trustiness of unmanned aerial vehicles, and their interactions with the vehicles and devices on the ground.

References

[1] Y. Wang and F. Li, "Vehicular ad hoc networks," in *Guide to Wireless Ad Hoc Networks*. London, U.K.: Springer, 2009, pp. 503–525. AQ4

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

[3] O. Kaiwartya *et al.*, "Internet of Vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[4] S. Mumtaz *et al.*, "Cognitive vehicular communication for 5G," *IEEE Commun. Mag.*, vol. 53, no. 7, pp. 109–117, Jul. 2015.

[5] R. Levien and A. Aiken, "Attack-resistant trust metrics for public key certification," in *Proc. Usenix Security*, 1998, p. 18.

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

[7] T. DuBois, J. Golbeck, and A. Srinivasan, "Predicting trust and distrust in social networks," in *Proc. IEEE 3rd Int. Conf. Privacy Security Risk Trust (PASSAT) Soc. Comput. (SocialCom)*, 2011, pp. 418–424.

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

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

[10] J. Zhang, "A survey on trust management for VANETs," in *Proc. IEEE It. Conf. Adv. Inf. Netw. Appl. (AINA)*, 2011, pp. 105–112.

[11] N. Yang, "A similarity based trust and reputation management framework for VANETs," *Int. J. Future Gener. Commun. Netw.*, vol. 6, no. 2, pp. 25–34, 2013.

[12] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "Trust and exclusion in vehicular ad hoc networks: An economic incentive model based approach," in *Proc. Comput. Commun. IT Appl. Conf. (ComComAp)*, 2013, pp. 13–18.

[13] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *Proc. Int. Conf. Netw. Syst. Security*, 2013, pp. 94–108.

[14] 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," *Veh. Commun.*, vol. 9, pp. 254–267, Jul. 2017.

[15] 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," *Comput. Commun.*, vol. 93, pp. 68–83, Nov. 2016.

[16] J. Contreras, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of Vehicles: Architecture, protocols, and security," *IEEE Internet Things J.*, to be published. AQ5

[17] M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: A trustworthy forensic investigation framework for the Internet of Vehicles (IoV)," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, 2017, pp. 25–32.

[18] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Trust on the Ratee: A trust management system for social Internet of Vehicles," *Wireless Commun. Mobile Comput.*, vol. 2017, Dec. 2017, Art. no. 7089259. AQ6

[19] 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.

[20] A. M. Vegni and V. Loscri, "A survey on vehicular social networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2397–2419, 4th Quart., 2015.

[21] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2377–2396, 4th Quart., 2015.

[22] P. Lytrivis, G. Thomaidis, M. Tsogas, and A. Amditis, "An advanced cooperative path prediction algorithm for safety applications in vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 669–679, Sep. 2011.

[23] P. Bergamo, P. D'Arco, A. De Santis, and L. Kocarev, "Security of public-key cryptosystems based on Chebyshev polynomials," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 52, no. 7, pp. 1382–1393, Jul. 2005.

[24] L. R. Ford and D. R. Fulkerson, "Maximal flow through a network," *Can. J. Math.*, vol. 8, no. 3, pp. 399–404, 1956.

[25] S. Al-Oufi, H.-N. Kim, and A. El Saddik, "A group trust metric for identifying people of trust in online social networks," *Expert Syst. Appl.*, vol. 39, no. 18, pp. 13173–13181, 2012.

[26] J. Leskovec, D. Huttenlocher, and J. Kleinberg, "Signed networks in social media," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2010, pp. 1361–1370.

[27] F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, "CityMob: A mobility model pattern generator for VANETs," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, 2008, pp. 370–374.

[28] 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 Inf. Syst.*, vol. 2016, Mar. 2016, Art. no. 5254141.