A Reputation-based Trustworthiness Concept for Wireless Networking in Vehicular Social Networks

Anna Maria Vegni, Claudia Leoni, Valeria Loscri, Abderrahim Benslimane

A Reputation-based Trustworthiness Concept for Wireless Networking in Vehicular Social Networks

Anna Maria Vegni, *Senior Member, IEEE,* Claudia Leoni, Valeria Loscrí, *Senior Member, IEEE,* and Abderrahim Benslimane, *Senior Member, IEEE*

***Abstract*—Social features are affecting different application areas, from traditional online social networks to economical networks, as well as the study of epidemical behaviors of pandemics and diseases. From the information point of view, also the Internet paradigm has been revised according to social behaviors of nodes, showing intrinsic properties that have allowed the definition of the Social Internet of Things paradigm. Furthermore, considering vehicular networks, social features have been spreading their influence, and defined the concept of Vehicular Social Networks, where mobile nodes show predictable social behavior. In this context, all the networking concepts should be updated accordingly, taking into account node social aspects and interactions. In this paper, we discuss the open challenge of how we should define a trust vehicle, relying on social networking aspects. We introduce the concept of node trustworthiness in a vehicular environment, based on the reputation degree, computed according to real-time interactions and past data. A node can be defined as trusted if exhibiting an acceptable reputation degree, and being successfully able to transmit data packet in a given environment. The framework of a network architecture for the computation of node trustworthiness degree in a vehicular scenario is also presented.**

***Index Terms*—Trustworthiness, social features, reputation degree, Vehicular Social Networks**

I. Introduction

The concept of vehicular networks has arisen from several years, carrying out a huge amount of research papers dealing with different challenging issues, from message propagation to connectivity holes, as well as reliability and security issues. It has been also noted that vehicular networks behave differently from traditional mobile wireless networks, following mobility constraints, and the reproducibility of mobility pattern allows to predict the traffic flow in a very accurate manner. Indeed, nodes in a vehicular network exhibit social attributes, just like humans do, and relationships among vehicles can be built following known social features [1].

One of the main features of vehicular networks is the ability of disseminating data messages in a fast and opportunistic way, through connectivity links built *on-the-fly*. The selection of a next-hop forwarder should rely on a secure and trusted vehicle, able to carry and forward a data message. Similarly to what happens in online social networks, where malicious users can enter in a user clique without approval, thus accessing to private information and data, also in vehicular networks malicious nodes are an issue. The detection of a malicious node should occur on the basis of the behavior of these nodes, both in the present and in the past experience, so that a bad behavior is an alert for a malicious node. For instance, a vehicle that is not reliable and fails in data forwarding, due to selfishness or lack of connectivity, should be avoided to be selected as next-hop forwarder. This behavior should be noted in the system, so that the vehicle trustworthiness degree is updated accordingly. Similarly, trusted vehicles should be "positively known", in order to be selected for data forwarding in a trusted and reliable manner.

How to define the node trustworthiness degree is still an open issue. Indeed, there exist several definitions previously proposed, mostly based on past and present node behavior and interactions (*i.e.*, social features). The concept of trustworthiness has been initially applied to social networks to detect trusted users [2], and recently extended to Industrial Internet of Things (IIoT) [3], where social industrial relationships, cooperation rate, direct and indirect honesty rate are exploited to manage trust. In [4] Shen *et al.* present a trustworthiness evaluation-based routing protocol, where the vehicle trustworthiness degree is calculated by the cloud depending on the vehicle attribute parameters.

In this paper, we provide a discussion on the concept of node trustworthiness in vehicular context, relying on both social features such as the node reputation degree, and on the node ability of data forwarding, such as the successful transmission probability. The latter concept is very relevant for the definition of a trusted node, since it is expected that such a node not only forwards secure information, but does so in successful way without errors and packet loss.

This paper is organized as follows. Section II presents an overview of different graph theory metrics used for defining the node trustworthiness degree. Particular attention will be focused to the vehicular scenario, where nodes move following known or expected mobility patterns. Furthermore, node mobility is ruled by social behavior, as typical of Vehicular Social Networks (VSNs), where nodes behave following social trends [1]. In Section III we investigate the concept of node trustworthiness degree, expressed in terms of successful transmission probability and reputation degree. The latter is a graph theory metric, based on friendship degree that exists among a pair of nodes. Section IV presents a social-based network architecture, adopted for the computation of the reputation-based trustworthiness degree. Numerical results are carried out in Section V, where the behavior of the reputation-based trust-

A.M. Vegni and C. Leoni are with Roma Tre University, Italy. Email: annamaria.vegni@uniroma3.it, cla.leoni5@stud.uniroma3.it.

V. Loscrí is with INRIA Lille-Nord Europe, France. Email: valeria.loscri@inria.fr.

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

worthiness degree is analysed for different environments and social features. Finally, an open discussion and conclusions are drawn at the end of the paper.

II. Graph theory metrics

There is no a unique definition of node trustworthiness, but depends on different disciplines. For instance, in wireless networking, the main goal is to design a secure system able to face any unexpected vulnerabilities, where a node is considered as trusted if still able to deliver data packets in a secure way. Sagar *et al.* [5] present a survey on trustworthiness in social IoT, and consider different metrics useful to define the node trustworthiness. In general, trust metrics refer to multiple features, ranging from node's social trust metrics to the quality of service (QoS) trust metrics, that are chosen and combined for trust purposes.

The social trust metrics represent the social behaviour of nodes in terms of the social relationships and is measured using integrity, benevolence, honesty, friendship, community-of-interest, and unselfishness. In general, in a social network, few nodes show a high social degree, while most have a lower one. This reflects the $80/20$ rule of power-law distribution [6]. On the other side, QoS metrics represent the ability that a node is able to offer a given QoS level and is measured in terms of reliability, data delivery ratio, throughput, and outage probability. However, the definition of node trustworthiness cannot rely on a single trust metric, but can also extend to joint criteria, *e.g.*, combining multitude of factors like both social and QoS metrics to form a single trust score.

In a social network, nodes present specific features that make them unique and are classified in different categories, according to the existing social ties among nodes, that can be weak and strong ties. As a result, nodes in a social network have different importance and play specific roles. For instance, for data dissemination purpose, the selection of a central node as packet forwarder allows to enhance network performance. Indeed, it has been observed that the definition of central node is sometimes adopted to define a social node, assuming that the social degree of a node refers to the probability that it is "socially active" [7], and then is able to share data packets in the network. A central node is likely to have a high social degree, since it can potentially reach a huge portion of nodes in the network. However, a node with a high social degree is not necessarily a central node. A node interested in the content produced and inter-changed among members in that specific network can gain the role of social node, even if does not play as central one. This issue also applies to selfish central nodes, which do not act as social nodes while potentially being so.

Numerous studies show that social networks are mostly scale-free networks in which the number of contacts is not distributed homogeneously across all members, and are made up of many scarcely interconnected and only some highly integrated members, the so-called hubs [7]. These hubs act as a link between individual groups of strongly interconnected members. In order to identify these hub nodes, it appears appropriate to make use of centrality metrics that have been developed within the Social Network Analysis (SNA) [6]. Ceolin and Potenza [8] introduce five metrics for measuring trust, from degree centrality to the eigenvector centrality, and it is estimated based on the user activity. They analyse the use of network centrality measures to predict trusted nodes, and it is observed that the more central a node is, the more prone to trust other nodes will be. The use of graph metrics for trustworthiness management has been also adopted in [9]. The authors introduce two different types of trust degree *i.e.*, familiarity trust and similarity trust, which allow to consider different features of trustworthiness.

Moving from IoT to Internet of Vehicles (IoV), the trustworthiness concept still plays a vital role, since it facilitates data sharing among vehicles, to achieve better driving safety and convenience. Without trustworthiness assessment, a vehicle may not be able to trust other vehicles, and therefore simply drop the data shared from others, to avoid potential driving dangers. There are several approaches for the computation of the node trustworthiness in vehicular networks [10], distinguishing among decision, evaluation, and management models. In the case of evaluation models, there are techniques relying on fuzzy logic, heuristic approaches, and statistical models. The trust of a node is computed according to different attributes, and usually involve social features [11] and QoS trust. About social features, usually a central node is the preferred next-hop forwarder for packet dissemination in IoV, due to its high centrality degree. Indeed, a central node is expected to forward packets to the highest number of neighboring nodes, as well as is able to connect separated clusters of vehicles, and sometimes acts as bridging node in a sparse scenario. In [7], a node is central if the number of direct connections to its neighbors (*i.e.*, node degree) is the highest in the network. This definition corresponds to a hub node that is also a central node.

III. Node Trustworthiness Degree

Trustworthiness is a key concept in critical infrastructures in the context of future wireless systems, since it enables the design of new approaches based on the expected behavior and outcomes of the system. In practice, if we are able to define trust metrics, we can exploit these metrics to characterize behaviors that are outside the expected perimeter and can depend on unintentional fault or intentional attacks. With this aim, in this work we focus on the technical characterization of trustworthiness in a dynamic and critical infrastructure.

The "position" of a trusted node within the network plays an important role that may affect the network performance. Indeed, if a central node is not trusted it is expected to negatively damage the packet forwarding within the network, while if a node with low centrality degree is not trusted, the network performance will be likely not damaged. On the other side, a trusted and central node is expected to enhance network performance. This approach describes the social-based trustworthiness degree, which assumes that the i-th node is trusted if, apart the probability of successful packet transmission, it has a high social degree, that depends on its transmission activity within the network. This is strictly dependent on the node itself and does not change for different propagation

environments. The node social degree is an intrinsic feature, acquired based on node's behavior in the past and present time intervals.

In this paper, we introduce a different definition for the node trustworthiness degree, which exploits the concept of node reputation degree that is an intrinsic node feature that depends on the analysis of network graph. However, in order to nominate a node as a trusted one, this is expected to not only show a high trustworthiness degree, but there are some conditions that can limit and make it a not-trusted node. It results important to evaluate the successful data transmission probability (*i.e.*, the outage probability), which depends on the particular propagation scenario for a given interference level. Specifically, an environment affected by high interference and noise will result in a reduction of the successful data transmission probability, and as a consequence the node trustworthiness degree will decrease. It can be observed that the proposed approach is similar to other existing works that exploit the concept of contract theory, mainly for data acquisition and trust management in social IoT [12], [13]. Specifically, in [12] both social and physical features of nodes in SIoT are analyzed to define the nodes' unique types, while in [13] the authors exploit the principles of network economics for trust management based on the efforts of node neighbors.

Different from [12], [13], in this paper we exploit the successful transmission probability achievable in a vehicular environment, which depends on the outage probability that is affected by the propagation environment, the transmission modes *i.e.*, Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I), and the level of interference. In our network scenario, we assume vehicles communicate to each other via V2V dedicated short range communications. Different vehicular scenarios require the transport of data messages with different performance requirements for the 3GPP system. From [14], we have considered three different environments *i.e.*, (*i*) UrbanMicro (UMi), (*ii*) UrbanMacro (UMa), and (*iii*) Rural, and the radio transmission in case of Line of Sight (LoS) between vehicles (*i.e.*, V2V). Specifically, UMi refers to street canyon and open area, which are intended to real-life scenarios capture, such as a city or station square. On the other side, in UMa, cell coverage is extended to km-range, while the rural deployment scenario focuses on larger and continuous wide coverage, supporting high speed vehicles.

The successful transmission probability depends on physical parameters, such as the communication mode and the propagation environment, and shows the feasibility of a node to successfully transmit a packet in a given environment and following a given communication mode. Given the dinamicity of the vehicular network environment, this can be affected by the noise and interference level. Indeed, the successful data transmission probability is strictly correlated to the probability to correctly receive a packet, that is based on the Signal-to-Interference plus Noise power ratio, expected to be lower than a given threshold. Experienced SINRs depend on the propagation environment, the link budget parameters (*e.g.*, antenna gains and receiver chain losses), the distance between the transmitting vehicle and the receiver one, and the interference due to other simultaneous communications in the same bandwidth.

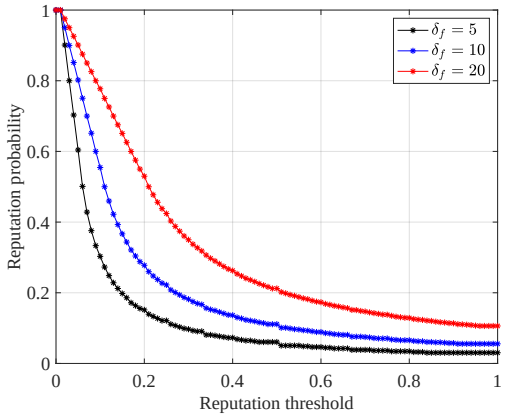

Fig. 1. Node reputation probability versus the reputation threshold, for different values of friendship degree, expressed as δ_f.

In the following Subsection we present our proposed definitions for the trustworthiness node degree.

A. Reputation-based Trustworthiness Degree

The reputation-based trustworthiness degree (RTD) concept assumes that the i-th node is trusted if (*i*) it exhibits a "high" probability of success in packet transmission, and also (*ii*) shows a high reputation node degree. The successful transmission probability of a node depends on the environment and physical parameters like the distance from a destination node. Of course, higher is the node successful transmission probability, higher will be its RTD, for a fixed reputation threshold. It is observed that for shorter distances in UMa and V2V transmission mode, the outage probability is reduced (*i.e.*, typical values range from 10^{-3} to 10^{-1}) and then the transmission will be more successful. The reputation-based trustworthiness node degree is then computed as the product of the successful transmission probability with the reputation degree.

The reputation node degree of the i-th node represents how much such a node is relevant for the j-th node, under the condition that both two nodes belong to the same network and are connected through a path. It is represented by the ratio between the number of nodes in common to the i-th and the j-th node, and the number of neighbors (*i.e.*, one-hop nodes) of the i-th node, that is, the node degree. This aspect is defined as "friendship degree", that is, it represents the number of common friends shared with another node.

The concept of reputation node degree is then used to compute the reputation probability, expressed as the probability that the i-th node has a reputation degree higher than a given threshold. The reputation probability depends on the threshold set as comparison purpose, as well as the friendship degree exhibited by a node. The reputation probability represents a requirement for secure communications. Higher is the reputation probability, higher will be the trustworthiness level to achieve. For a given service, the reputation threshold represents a user-defined trustworthiness requirement.

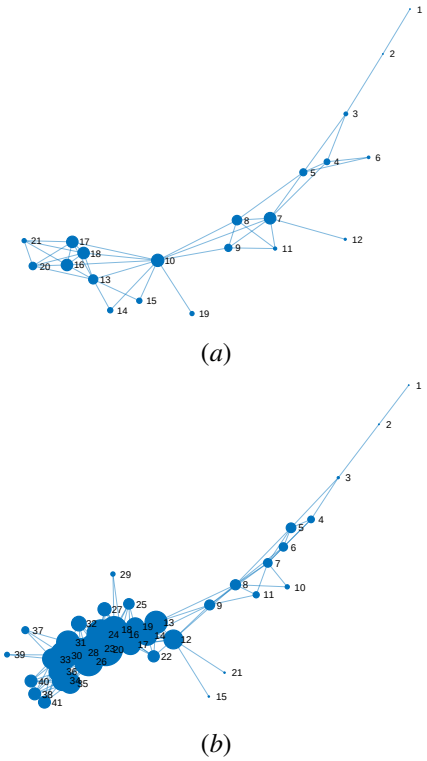

Fig. 2. Reputation graphs for (*a*) small and (*b*) large network size, respectively. The size of each node is proportional to the reputation degree.

Fig. 1 represents the analytical trend of the node reputation probability for different values of the friendship parameter, assuming the node degree is uniformly distributed from 1 to 100 within the network. We observe that for an increasing reputation threshold, the reputation probability of a node decreases, since a higher reputation threshold is desired and only a limited number of nodes can exhibit this requirement. Furthermore, for increasing values of the friendship degree, the reputation probability is higher for a fixed reputation threshold. Indeed, if the i-th node shows many common nodes with the j-th node (see for instance the *red* curve), then it is expected to get a higher reputation degree, as compared to the case of lower number of common nodes with the j-th node (see the *black* curve).

Fig. 2 shows the node reputation graph for different network sizes. The graphs were generated according to two sets of synthetic traces depicting a vehicular network behavior, in case of two scenarios, namely small and large size networks, each comprised of 21 and 41 nodes, with one node as a source vehicle and the remaining ones as potential forwarders, [15]. For nodes showing higher friendship degree (*i.e.*, larger number of common nodes), the reputation degree is higher, depicted as a circle whose size is proportional to the reputation degree. Notice that for nodes with limited number of neighbors (*i.e.*, one and two node degree), the reputation degree is low, since also their friendship degree is limited. On the other side, nodes more connected in the network, showing high friendship degree, will present a higher reputation degree. For instance, in Fig. 2 (*a*) node 10 is one of the most connected nodes, with a

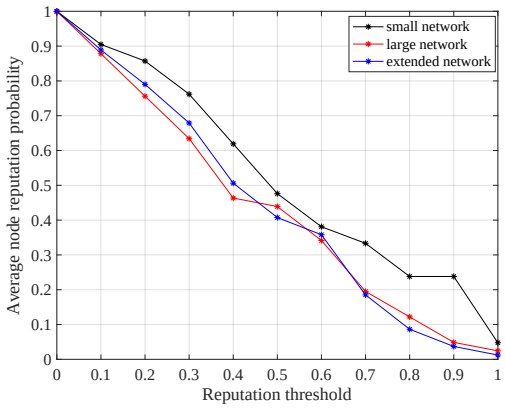

Fig. 3. Average reputation probability versus the reputation threshold, for different network sizes.

node degree of 10. Also, node 10 is connected to nodes 16, 17, and 18, who are also connected to node 21. So, nodes 21 and 10 are not directly connected, but share three friends. Higher is the friendship degree, higher will be the reputation degree. In contrast, node 4 shows a lower reputation degree, as it has a lower friendship degree. Indeed, node 4 is a common friend with nodes 2, 7, 8, 9, 10, 11, and 12. Similar considerations apply to the large network in Fig. 2 (*b*).

It should be noticed that, since the computation of the node reputation probability is based on the friendship degree, the reputation probability is independent from the global number of nodes in the network and just depends on the number of close friends. The behavior of the reputation probability in extended networks will still present a decreasing behavior for increasing reputation threshold. Fig. 3 compares the average reputation probability versus the reputation threshold in case of small, large and extended network size, corresponding to 21, 41 and 81 nodes, respectively. In all the cases, the reputation probability decreases for increasing reputation threshold but lower values are shown in case of higher network size. This behavior is due since in a small network nodes are expected to be more connected to each other and also the node friendship degree will be higher.

IV. Social-based Trustworthiness Network Architecture

According to the definition of RTD, nodes exhibiting higher friendship degree and having high node degree are potentially trusted nodes, upon considerations about the vehicular environment that can affect their transmission probability. In order to compute the RTD, it is assumed that nodes share graph information, according to the network architecture as depicted in Fig. 4.

The proposed architecture is aimed for the computation of the reputation-based trustworthiness degree, assuming a VSN environment. Let us assume a set of vehicles are moving along the road in a given environment (*i.e.*, UMi, UMa, and Rural). V2V communications among vehicles occur in opportunistic way whenever two vehicles are in short range. Vehicles are moving along the lanes following the Poisson spatial distribution and forming different-size clusters, each

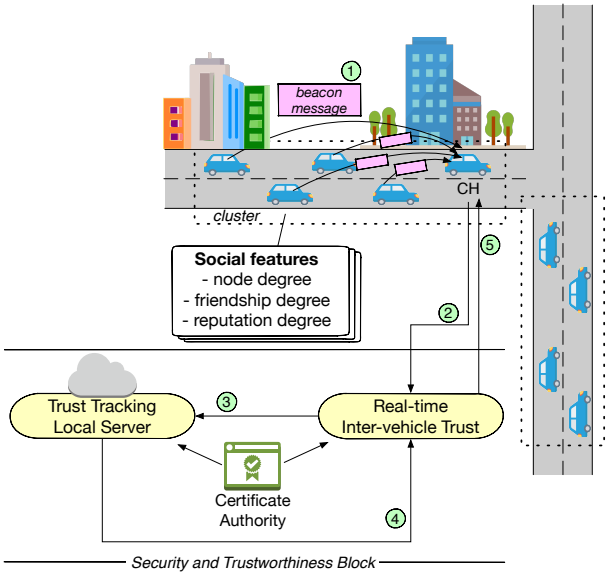

Fig. 4. Proposed social-based network architecture in vehicular environment.

of them lead by a Cluster Head (CH) responsible of the main operations in a cluster, such as data collection and mining, data forwarding, etc. If a vehicle in a cluster is willing to send a data packet in a secure way, it will be opportune to select a trust node as next-hop forwarder via V2V propagation mode. How to select a trusted forwarder within a cluster is the main goal of the CH. Indeed, the CH has information about the trustworthiness degree in the cluster, as well as the successful transmission probability for each node in the cluster, and such information can be shared among neighboring nodes. Once the information about trustworthiness degree is known to all the nodes in the cluster, secure and reliable communications are guaranteed by selecting the trust next-hop forwarder.

The node trustworthiness degree is computed by the CH according to (*i*) the node reputation probability and (*ii*) the successful transmission probability. The first parameter is set based on the reputation threshold, that expresses the level of reputation required. For instance, services requiring high trustworthiness will need a high reputation threshold. The successful transmission probability for a vehicle willing to send a data message mainly depends on the distance from a destination node. It follows that the final node trustworthiness degree is computed as the product of the successful transmission probability with the reputation degree, taking into account the reputation threshold and the distance to a destination node.

According to Fig. 4, each vehicle in a cluster shares its own social features and physical parameters with the CH by means of a beacon message (see point 1 in Fig. 4). Physical parameters (*e.g.*, the transmission power, position, antenna gain, noise level, etc.) are useful to compute the successful transmission probability in a given environment. Social features are intended in terms of node degree, friendship and reputation degree, computed in a synchronous time interval (*i.e.*, real-time measurements) and from past time windows (*i.e.*, historical data). Information about social features are collected by each node by means of SNA tools, that is, considering the distance, the centrality, the node degree, etc. In each beacon message, it is encoded the reputation degree of the sender vehicle, computed from SNA. Specifically, the reputation degree of the i-th node is computed from different contributions coming from close nodes.

The CH is responsible for the computation of the trustworthiness degree of each vehicle sending the beacon message. The trustworthiness degree of the i-th vehicle is computed based on its reputation degree, as well as taking into account the distance from the CH to the i-th vehicle [1]. The distance parameter is a relevant factor since it allows monitoring the message transmission from a potentially trusted vehicle *i.e.*, a node is trusted if it shows a high reputation degree, but also if able to successfully transmit a message flow. Based on the distance and the specific environment, the message propagation can suffer for interference, resulting in a bad connectivity link. It follows that furthest vehicle from the CH will experience a worst transmission quality, as compared to those vehicles closer to the CH.

The trustworthiness degree is addressed by different entities, *i.e.*, CH and certificate authorities (CA), that provide the trustworthiness degree to vehicles themselves. The security and trustworthiness block works on a twofold basis *i.e.*, (*i*) through real-time inter-vehicle interactions that recommend the vehicle's trust based on the interactions among vehicles (see point 2), and (*ii*) by means of a trust tracking local server that checks for the vehicle's past trustworthiness activities (*i.e.*, node historical data). Specifically, the real-time interactions refer to V2V message beacons to the CH, which are used to extract information about the node reputation probability and the successful transmission probability. We assume that the trustworthiness degree associated to each node in the cluster is timely stored in a local server, and updated accordingly if the value shows large variations. Notice that both two trustworthiness layers interact between each other, since the real-time trust engine sends updates on the vehicle trustworthiness information, previously stored in a local server (see point 3 in Fig. 4). At the same time, the trust tracking local server sends back corrections on the trustworthiness degree to the real-time inter-vehicle trust engine that relies on the CH (see point 4). For instance, if the gap between the trustworthiness degree computed in real-time and that one from past stores is too large, then the final trustworthiness degree will be updated according to the past informations. The output from the trustworthiness block is the list of the potential trusted vehicles (see point 5). The one on the top will be selected by the CH as "cluster trusted node", and will be given the role of next-hop forwarder.

We can observe that in the proposed social-based network architecture, data information and signaling overhead depends on the number of vehicles $(N-1)$ that comprise the cluster, as well as on $2M$ *i.e.*, with $M \leq N-1$, control packets from the CH to the trust tracking local server, and back, in case of variations of the node trustworthiness degree from the stored values. So, the overhead ranges from $(N-1)$ to $3(N-1)$, where N is typically a small value as for a cluster network.

[1]Information about node positioning is known through GPS technology.

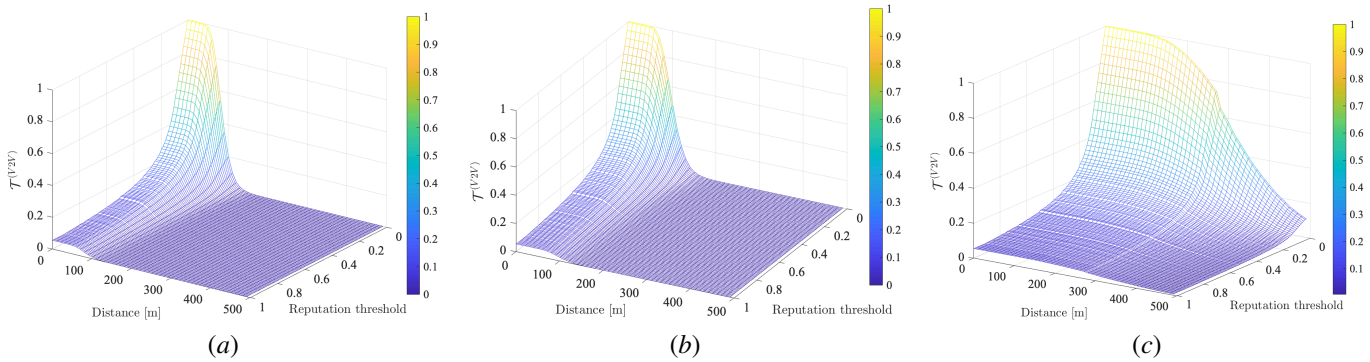

Fig. 5. Reputation-based trustworthiness node degree *i.e.*, $\mathcal{T}^{(V2V)}$, vs. the reputation threshold and the V2V communication distance, in case of (*a*) UrbanMicro, (*b*) UrbanMacro and (*c*) Rural scenario, respectively.

Specifically, for no variations of the node trustworthiness degree from the past values, the overhead will be $(N-1)$, while in case of variations it will be $(N-1)+2M = 3(N-1)$.

V. Numerical results

In this section we present the numerical results of the proposed *reputation-based* trustworthiness node degree, evaluated for different propagation scenarios assuming V2V communication mode. Specifically, we have considered three different environments *i.e.*, (*i*) UMi, (*ii*) UMa, and (*iii*) Rural, where the radio transmission occurs in case of LoS propagation with a low interference level (*i.e.*, noise raise of 5 dB), and vehicles are assumed to be connected via V2V. Numerical results have been carried out via MatLab simulator. Specifically, assuming the pathloss model from [14], for UMa we set the values of the transmitting power $P_t = 100$ [mW], the antenna gains [dB] for the vehicles (*i.e.*, $G_{veh} = 3$ dB), the height [m] of the vehicle (*i.e.*, $h_{veh} = 1.5$ m), the noise figure $F = 7$ [dB], the noise raise $I = 5$ [dB] due to other cell interference, the bandwidth $B = 10$ [MHz], the transmitting frequency $f_c = 5.9$ [GHz], and the SINR target $\rho = 12$ [dB]. Simulation results in case of UMi and Rural scenario can change accordingly.

Assuming the computation of the trustworthiness degree occurs according to the network architecture depicted in Fig. 4, we present the analytical trend of the node trustworthiness degree for different propagation environments. As for its definition, a given node shows a trustworthiness degree that depends on the communication distance from such vehicle to a destination one and on the reputation threshold. In Fig. 5, we can observe that for short distances *i.e.*, within ≈ 100 m for urban scenarios, the trustworthiness degree is higher than the case of longer distances, since the successful transmission probability shows a power-law profile. On the other side, for increasing values of the reputation threshold, the node trustworthiness degree will be decreasing, meaning that for more reputation requirement, lower will be the reputation probability and then, the trustworthiness degree. This result is in accordance to the previous trend of the reputation degree in Fig. 1.

It is worth noticing that although the dependence on the reputation degree is a feature of the node itself, the trustworthiness degree will suffer more in case of different propagation environments. Fig. 5 depicts the different trends of trustworthiness node degree, achieved in case of UrbanMicro, UrbanMacro, and Rural scenarios, assuming a given friendship degree *i.e.*, $\delta_f = 5$. It can be noticed the strong increase of the trustworthiness degree for longer distances in case of rural environment, as depicted in Fig. 5 (*c*). In this case, the trustworthiness degree distribution is no more concentrated in a narrow area for limited distance as occurring in Fig. 5 (*a*) and (*b*), but we observe a more spread distribution. This results in higher values of the trustworthiness degree in rural environment, since nodes experience a more successful propagation behavior and are poor affected by interference. Similarly, both the urban scenarios present the trustworthiness distribution in a limited area, thus resulting in a more stringent selection of trusted nodes. Indeed, it can be observed that in UMi and UMa the trustworthiness node degree is zero for distances higher than 100 m. This is due to the transmission probability that is affected by outage, resulting in bad transmission quality (*i.e.*, communication link not feasible). As a consequence, the trustworthiness node degree will be null in such conditions.

VI. Conclusions and open issues

This paper has investigated the node trustworthiness degree in vehicular networks. No unique definition for trustworthiness exists, but it depends on which criterium is assumed for its computation. It has been observed that the node social features are extremely important to define a trust node, especially in the context of vehicular networks. It has been shown how vehicular nodes are affected by social behaviors, as in case of mobility patterns. It follows that social features can provide useful information about the nature of a node, defining the node as malicious or not. In this paper, we have proposed a trustworthiness criterium based on both the node reputation degree, as well as on the successful transmission probability. The first parameter takes into account the number of "common friends" to other nodes, and the node degree. According to graph metrics, we have observed increasing reputation degrees for higher number of common friends. On the other side, the successful transmission probability depends on the vehicular scenario affected by interference and noise.

Leveraging on the above considerations, a social-based network architecture for node trustworthiness detection has been

presented. A trusted vehicle is selected based on both real-time measurements and past interactions. The vehicle exhibiting the highest trustworthiness degree will be selected as next-hop forwarder. We observed that in case of different environments, the trustworthiness degree varies, showing reduced values for short distances and higher reputation threshold.

As an open discussion, we need to investigate the dynamicity of graph theory metrics, such as centrality degree, which can be affected by fast variations especially in high dynamic environments. Solutions for predicting these metrics should rely on Machine Learning/Artificial Intelligence based techniques.

REFERENCES

[1] A. M. Vegni and V. Loscrí, "A Survey on Vehicular Social Networks," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2397–2419, 2015.

[2] M. Agarwal and B. Zhou, "Detecting Malicious Activities Using Backward Propagation of Trustworthiness over Heterogeneous Social Graph," in *2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)*, vol. 3, 2013, pp. 290–291.

[3] C. Boudagdigue, A. Benslimane, A. Kobbane, and J. Liu, "Trust Management in Industrial Internet of Things," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3667–3682, 2020.

[4] J. Shen, C. Wang, A. Castiglione, D. Liu, and C. Esposito, "Trustworthiness Evaluation-Based Routing Protocol for Incompletely Predictable Vehicular Ad Hoc Networks," *IEEE Transactions on Big Data*, vol. 8, no. 1, pp. 48–59, 2022.

[5] S. Sagar, A. Mahmood, Q. Z. Sheng, J. K. Pabani, and W. E. Zhang, "Understanding the Trustworthiness Management in the Social Internet of Things: A Survey," 2022. [Online]. Available: https://arxiv.org/abs/2202.03624

[6] A.-L. Barabasi, *Network Science*. Cambridge Univ. Press, 2016.

[7] A. M. Vegni, C. Souza, V. Loscrí, E. Hernández-Orallo, and P. Manzoni, "Data Transmissions Using Hub Nodes in Vehicular Social Networks," *IEEE Transactions on Mobile Computing*, vol. 19, no. 7, pp. 1570–1585, 2020.

[8] D. Ceolin and S. Potenza, "Social Network Analysis for Trust Prediction," in *11th IFIP International Conference on Trust Management (TM)*, ser. Trust Management XI, J.-P. Steghöfer and B. Esfandiari, Eds., vol. AICT-505. Gothenburg, Sweden: Springer International Publishing, Jun. 2017, pp. 49–56, part 2: Novel Sources of Trust and Trust Information. [Online]. Available: https://hal.inria.fr/hal-01651167

[9] H. Xia, F. Xiao, S.-s. Zhang, C.-q. Hu, and X.-z. Cheng, "Trustworthiness Inference Framework in the Social Internet of Things: A Context-Aware Approach," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019, pp. 838–846.

[10] J. Wang, Z. Yan, H. Wang, T. Li, and W. Pedrycz, "A Survey on Trust Models in Heterogeneous Networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2127–2162, 2022.

[11] Q. Yang and H. Wang, "Toward trustworthy vehicular social networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 42–47, 2015.

[12] F. Sangoleye, N. Irtija, and E. E. Tsiropoulou, "Data Acquisition in Social Internet of Things based on Contract Theory," in *ICC 2021 - IEEE International Conference on Communications*, 2021, pp. 1–6.

[13] G. Fragkos, C. Minwalla, J. Plusquellic, and E. E. Tsiropoulou, "Local Trust in Internet of Things Based on Contract Theory," *Sensors*, vol. 22, no. 6, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/6/2393

[14] "Study on channel model for frequencies from 0.5 to 100 GHz," ETSI Technical Report, 3GPP TR 38.901 version 14.3.0 Release 14, Tech. Rep., 2018.

[15] A. M. Vegni, V. Loscrí, and P. Manzoni, "Data Forwarding Techniques Based on Graph Theory Metrics in Vehicular Social Networks," in *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2018, pp. 1771–1775.

Anna Maria Vegni (Senior member, IEEE) is Associate Professor in Telecommunications at Roma Tre University (Rome, Italy), since March 2023. She received the Ph.D. degree in Biomedical Engineering, Electromagnetics and Telecommunications from the Department of Applied Electronics, Roma Tre University, in March 2010. In 2009, she was a visiting researcher in the Multimedia Communication Laboratory, directed by Prof. Thomas D.C. Little, Boston University, Boston, MA. Her research activity focus on vehicular networking, RF and optical wireless communications. She is involved in the organization of several IEEE and ACM international conferences and is a member of the editorial board of IEEE Communications Magazine, IEEE TCOM, Ad Hoc Networks, Journal of Networks and Computer Applications Elsevier journals, WINET Springer, IEEE JCN, ITU J-FET and ETT Wiley journal.

Claudia Leoni is a student pursuing her master's degree in Telecommunications at the Department of Industrial, Electronic and Mechanical Engineering, Roma Tre University. She got her B.Sc. degree in Electronics Engineering from the same university in December 2022. Among her initial research interests, she is actively engaged in studying vehicular networks and social networking.

Valeria Loscrí is a permanent researcher of the FUN Team at Inria Lille–Nord Europe since Oct. 2013. From Dec. 2006 to Sept. 2013, she was Research Fellow in the TITAN Lab of the University of Calabria, Italy. She received her MSc and PhD degrees in Computer Science in 2003 and 2007, respectively, from the University of Calabria and her HDR (Habilitation á diriger des recherches) in 2018 from Université de Lille (France). Her research interests focus on emerging technologies for new communication paradigms such as VLC and Tera-Hertz bandwidth and cooperation and coexistence of wireless heterogeneous devices. She has been involved in the activity of several European Projects (H2020 CyberSANE, FP7 EU project VITAL, the FP6 EU project MASCOT, etc.). She is in the editorial board of IEEE COMST, Elsevier ComNet, JNCA, IEEE Trans. Nanobioscience. Since 2019, she is Scientific International Delegate for Inria Lille–Nord Europe.

Abderrahim Benslimane is Full Professor of Computer-Science at the Avignon University/France since 2001. He is Vice Dean of the Faculty of Sciences and Technology and Head of the master?s degree SICOM, Communicating Systems. He has been nominated in 2020 and renewed in 2022 as IEEE VTS Distinguished Lecturer. He has been as Associate Professor at the University of Technology of Belfort-Montbeliard since September 1994. He obtained the title to supervise research (HDR 2000) from the University of Cergy-Pontoise, France. He received the PhD degree (1993), DEA (MS 1989) from the Franche-Comte University of Besancon, and BS (1987) from the University of Nancy, all in Computer Science. He was Board committee member, Vice-chair of Student activities of IEEE France section/Region 8; he was Publication Vice-chair and Conference Vice-Chair of the ComSoc TC of Communication and Information Security. He supervised more than 22 Ph.D thesis and more than 42 M.Sc. research thesis. For more detail, see my complete CV: http://abderrahimbenslimane.org/