Reputation-based Trustworthiness Degree in Interference-variable Vehicular Networks

Claudia Leoni*, Anna Maria Vegni*, Valeria Loscrí†, and Abderrahim Benslimane‡
*Dept. of Industrial, Electronic and Mechanical Engineering, Roma Tre University, Italy
cla.leoni5@stud.uniroma3.it, annamaria.vegni@uniroma3.it
†Inria Lille-Nord Europe, France, valeria.loscri@inria.fr
‡University of Avignon, France, abderrahim.benslimane@univ-avignon.fr

***Abstract*—Trustworthiness in wireless networks is an open challenge due to several features that should be taken into account. All the networking concepts should be updated accordingly, as well as physical layer features that influence the node transmission ability. Indeed, a trusted vehicle is expected to efficiently forward data packets, in order to reach the highest number of neighbors. At the same time, a trusted vehicle is expected to be well-recognized within the network, thanks to a high reputation degree. In this paper, we discuss the open challenge of trustworthiness node degree, based on both the reputation degree computed according to real-time interactions and past data, and on physical features of the wireless communication channel. 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. However, the node trustworthiness degree is also strongly affected by the interference level in the reference scenario. Indeed, interfering nodes can negatively influence the node reputation degree, causing a decrease of the trustworthiness node degree.**

***Index Terms*—Trustworthiness, reputation, vehicular networks, outage probability.**

I. Introduction

Since several decades, vehicular ad-hoc networks have been established as a well-known technology, addressing various aspects from physical features to networking aspects, such as message transmission, connectivity holes, reliability, as well as security threats [1]. Despite vehicular networks behave differently from traditional mobile ad-hoc networks, it is possible to predict their behavior thanks to social features of nodes [2]. Additionally, it is possible to accurately reproduce mobility patterns, allowing precise prediction of traffic flow, as well as optimize content dissemination through the social networking features [3].

Security in vehicular networks is essential to select the most appropriate next-hop forwarder, which is expected to be the most reliable and secure. Identifying malicious nodes occurs by observing vehicle's behavior in relation to other network nodes, based on both present and past interactions. If a vehicle displays negative behavior, it is likely a malicious node. In other words, if a node is unreliable or fails to transmit data due to connectivity issues or selfishness, it will be avoided when selecting the next forwarder. This behavior must be tracked to keep the node's trustworthiness updated. At the same time, it is crucial to identify vehicles that send data securely and reliably.

Trustworthiness in vehicular networks is paramount for ensuring the safety and efficiency of data forwarding between vehicles and from vehicles to the infrastructure. The trustworthiness degree of a node is something that is still being studied, and there are several definitions regarding it, most of which are based on the present and past interactions between vehicles and their behavior in the network. In general, the trustworthiness degree involves several aspects, including data integrity, privacy, and authentication. Indeed, a trust node should guarantee that data transmitted within the vehicular network remains unaltered and authentic. This is accomplished by verifying the identity of vehicles, and guaranteeing high node reputation degree.

Vehicular networks are susceptible to various types of attacks, including spoofing, jamming, and man-in-the-middle attacks. Trusted nodes represent robust security measures, which are able to detect and effectively mitigate such vehicular threats. Overall, ensuring trustworthiness in vehicular networks requires a holistic approach that addresses both technical and social features of security and privacy. This paper investigates the concept of trustworthiness in vehicular networks, taking into account (*i*) the node reputation degree and (*ii*) the ability to successfully transmit data within the network. Both aspects are expected to be strongly affected by the interference level in the network [4]. Interfering nodes can disrupt communication and pose significant challenges to the reliability and efficiency of the network. For instance, some nodes may intentionally interfere with communication in vehicular networks to disrupt traffic flow, compromise safety messages, or launch attacks [5]. Interference can also occur due to unintentional sources, such as malfunctioning equip-

ISBN 978-3-903176-63-8 ©2024 IFIP

ment, electromagnetic interference from nearby devices, or environmental factors. Although such nodes are not malicious in nature, they can still disrupt communication and affect the overall performance of the network. Then, inefficient communications due to interference can also impact the reliability of services like traffic management and navigation. For all these reasons, it is necessary to consider dynamic scenarios where the impact of interfering nodes can influence network performance.

The rest of this paper is organized as follows. Section II presents some recent works dealing with trustworthiness in wireless networks, and in particular vehicular networks. In Section III we present our concept of trustworthiness node degree, based on both node reputation and successful transmission probability. Simulation results are then presented in Section IV in order to assess the proposed trustworthiness degree in different vehicular scenarios and interference levels. The dependence of trustworthiness on specific environments is evinced, and different trends are shown for variable distance, reputation degree, and interference level. Finally, conclusions are drawn at the end of the paper.

II. Related Works

Data trustworthiness represents the "correctness" of data originated by a certain source. Indeed, data has to be computed reliable or trustworthy before being propagated in the network [6]. However, there exist several different ways to define trustworthiness. One of the first definition is related to social networks, and it is considered in this context to detect trusted users [7], and recently extended to Industrial Internet of Things (IIoT) [8], where social industrial relationships, cooperation rate, direct and indirect honesty rate are exploited to manage trust. Also, data reliability is strictly connected to data trustworthiness and needs to be taken into account [9].

The node reputation degree is often tied to the trustworthiness concept, and usually it is computed based on past interactions of a given node with its neighbors. Trust aggregation refers to aggregating trust evidence collected through either self-observations or feedback from neighboring nodes. Neville and Shailaja [9] build a voting-based trustworthiness model. Also in this case, the node trustworthiness is computed based on the concepts of reputation and experience. This latter is determined by how frequently a node interacts with other nodes in the network.

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 [10]. Without the trustworthiness assessment, a vehicle may not be able to trust other vehicles, and therefore simply drop the data shared from untrusted vehicles.

There are several approaches for the computation of the node trustworthiness in vehicular networks [11], 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 and QoS trust [12]. In [13], a trust and reputation mechanism is proposed, able to separate malicious vehicles from the ideal ones. Specifically, the reputation is computed by combining direct and indirect trust opinions, while handling uncertainty associated with them. In [14] 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 [15], we investigated the concept of node trustworthiness, based on both physical features and node reputation, considering a low interference level.

Differently from previous works that focus the concept of trustworthiness on specific node features, such as the reputation degree, in this paper we extend to other important aspects, like the variable interference level of the propagation medium. Taking into account the results from [15], we investigate the dependence on the interference level that can affect the successful transmission probability, and then pose significant challenges to the reliability and efficiency of the vehicular network.

III. Reputation-based Trustworthiness Technique

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 Urban Macro (UMa) and Vehicle-to-Vehicle (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.

Let us assume a vehicular network comprised of $N \in \mathbb{Z}^+$ nodes. Given a pair of vehicles (*i.e.*, vehicle i and j), 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 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, a.k.a. friend nodes, and the number of neighbors (*i.e.*, one-hop nodes) of the i-th node *i.e.*,

$$R_{i,j} = \frac{\delta_{f,(i,j)}}{\delta_i}, \tag{1}$$

where δ_i is the degree of the i-th node, and $\delta_{f,(i,j)}$ is defined as "friendship degree", that represents the number of friends of the i-th node shared with the j-th node. Notice that Eq. (1) is for a given pair of nodes (i, j), while the reputation degree of the i-th node w.r.t the whole network of size N will be:

$$R_i = \frac{\sum_{j,j\neq i}^{N} \delta_{f,(i,j)}}{\delta_i}, \tag{2}$$

where we can pose $\sum_{j,j\neq i}^{N} \delta_{f,(i,j)} = \delta_f$ for simplicity. Notice that in our proposed concept of reputation, isolated nodes (*i.e.*, $\delta_i = 0$) are not considered.

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, namely r_{th}. The reputation probability of the i-th node depends on the threshold r_{th}, set as comparison purpose, as well as the friendship degree exhibited by the i-th 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.

The successful transmission probability for the i-th vehicle communicating in V2V mode is defined as follows:

$$\mathcal{P}_{succ,(i,j)}^{(V2V)} = 1 - P_{out,(i,j)}, \tag{3}$$

where $P_{out,i}$ is the outage probability associated to the i-th vehicle, and it is expressed as

$$P_{out,(i,j)} = \Pr\{SINR_{(i,j)} < \rho_0\}, \tag{4}$$

with $SINR_i$ as the Signal-to-Interference plus Noise ratio for the (i, j)-V2V link, given as

$$SINR_{(i,j)} = \frac{P_{Tx,i} \cdot G_{Tx,i} G_{Rx,j}}{\mathcal{L} \cdot (\eta + \mathcal{I})}, \tag{5}$$

where $P_{Tx,i}$ [W] is the transmitting power of the i-th vehicle, $G_{Tx,i}$ and G_{Rx} are the antenna gains for the transmitter and the receiver, respectively, $\mathcal{L}$ [dB] is the pathloss accounting for the losses due to the distance $d_{i,j}$ [m] between the i-th transmitting node and the j-th receiver node, η [W] is the thermal noise power, and $\mathcal{I}$ [dB] is the extra interference due to other simultaneous communications occurring in the same Physical Resource Blocks (PRBs). Also, in Eq. (4), ρ_0 is the SINR threshold for the considered service. Notice that the successful transmission probability is mainly affected by the inter-vehicle distance $d_{i,j}$ [m], the interference level $\mathcal{I}$, which is a feature of the reference environment, as well as the communication mode (specifically, vehicle-to-vehicle).

From the expression of the reputation node degree in Eq. (2) and the successful transmission probability in Eq. (3), we can derive the trustworthiness degree of the i-th node *i.e.*, $\mathcal{T}_i$, as

$$\mathcal{T}_i = \mathcal{P}_{succ,(i,j)}^{(V2V)} \cdot R_i. \tag{6}$$

Algorithm 1 presents the main steps for the computation of RTD, assuming a set $\mathcal{N}$ of nodes in a vehicular network for a given reference scenario. After computing the trustworthiness degree as in Eq. (6), a list of potentially trusted nodes is created and finally

Algorithm 1: Pseudocode for RTD

Input: Reference scenario ▷ UMi, UMa, Rural
$\mathcal{N} = [n_1, \ldots, n_i, \ldots, n_N],\ N \in \mathbb{Z}^+$ ▷ Set of vehicles
r_{th} ▷ Reputation threshold
$\mathcal{I}$ [dB] ▷ Interference level
d [m] ▷ Inter-vehicle distance
ξ ▷ Trustworthiness Threshold
t [ms] ▷ Trustworthiness update time
Output: $\mathcal{T}$ ▷ Trustworthiness node degree
L ▷ List of trusted nodes
f ▷ Next-hop trusted forwarder

Procedure `proc`(*Trustworthiness computation, t*)
  foreach $n_{i,j} \in \mathcal{N}$ **do**
    Compute R_i ▷ Eq. (2)
    Compute $\mathcal{P}_{succ,(i,j)}^{(V2V)}$ ▷ Eq. (3)
    Compute $\mathcal{T}_i$ ▷ Eq. (6)
  $L = [\mathcal{T}_1, \ldots, \mathcal{T}_i, \ldots, \mathcal{T}_N] | \mathcal{T}_1 \geq \mathcal{T}_i \geq \cdots \geq \mathcal{T}_N$ ▷ Sorted list of trusted nodes
  return L
foreach *pkt to send* **do**
  Procedure `proc`(*next-hop node selection*)
    if $\mathcal{T}_1 < \xi$ **then**
      $L = [\,]$ ▷ No node is trusted
      `proc`(*Trustworthiness computation, t*)
    else
      $f = n_i | \{\mathcal{T}_i = \mathcal{T}_1\}$ ▷ Trusted forwarder selected
    return f

sorted according to the highest value of trustworthiness degree. The trusted node selection criteria occurs according to a trustworthiness threshold (*i.e.*, ξ). The i-th node exhibiting the highest trustworthiness degree, under the condition $\mathcal{T}_i > \xi$, will be selected as next-hop trusted forwarder. On the other hand, if no node presents a trustworthiness degree higher than the threshold ξ, then the list of potential trusted nodes will be null and no node will be selected as trusted forwarder. The computation of the trustworthiness node degree will be repeated every t [ms], that represents an update time interval.

IV. Simulation Results

This section presents the numerical results achieved for the proposed trustworthiness concept. In our simulations, we assume a vehicular network scenario where vehicles are in V2V connectivity. We also consider different environments *i.e.*, (*i*) UrbanMicro (UMi), (*ii*) UMa, and (*iii*) Rural, where the radio transmission occurs in case of LoS propagation model, and for a variable interference level. Indeed, the noise raise is assumed varying from 5 dB to 10 dB for low and high interference level, respectively.

Numerical results have been carried out via MatLab simulator. The main simulation parameters are as in [15], where 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 $\mathcal{I} = 5$ dB due to other cell interference, the bandwidth $B = 10$ MHz, the transmitting frequency $f = 5.9$ GHz, and the SINR target $\rho_0 = 12$ dB. Furthermore, we assume a random distribution of node degree δ in the range $[1, 100]$, and different values of friendship degree *i.e.*, $\delta_f = [5, 10, 20]$.

The successful transmission probability is depicted in Fig. 1, where different trends are reported in case of different environments and variable interference level. This probability is evaluated versus the inter-vehicle distance, assuming vehicles are in V2V connectivity links. We notice high values are achieved in rural environment, where a successful probability of 0.9 is reached at a distance of 200 m in case of low interference, while for the same distance the probability is reduced to 0.55 in case of higher interference level. Similar values are obtained in case of UMi and UMa but for lower distances, approximately < 100 m.

From the results in Fig. 1, we can derive the behavior of the trustworthiness node degree, by assuming different values of the reputation threshold *i.e.*, $r_{th} = [0, 0.2, 0.5, 1]$, low and high interference level, as well as different friendship degree values. Fig. 2 presents the trustworthiness degree of a given node versus the

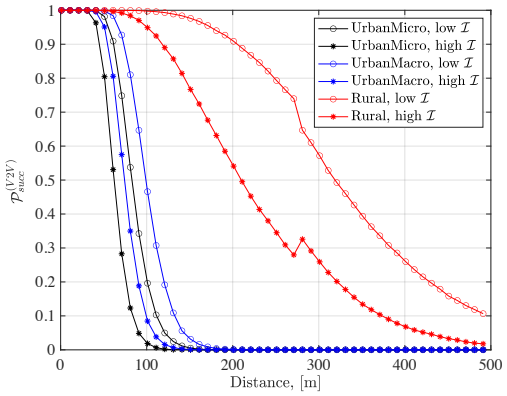
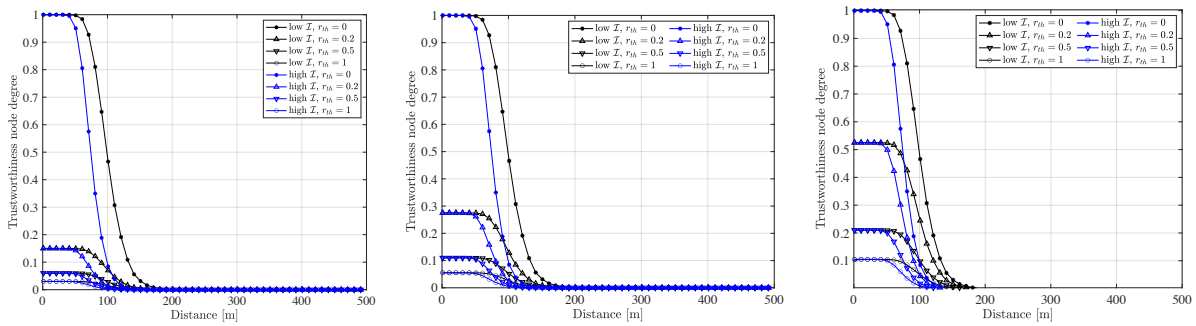


Fig. 1. Successful transmission probability vs. the vehicle inter-distance, in case of V2V connectivity for different scenarios and interference levels.

inter-vehicle distance, in case of UMa scenario. We observe that for increasing friendship degree $\delta_{f,(i,j)}$ the trustworthiness degree of node i is higher, while maintaining a decreasing trend for higher distances. This is an expected result, as for high values of the friendship node degree the i-th node will show high reputation degree. Furthermore, according to the reputation threshold r_{th}, the trustworthiness node degree will be reduced when $r_{th} \to 1$. This is an expected result as the reputation probability decreases for increasing reputation threshold.

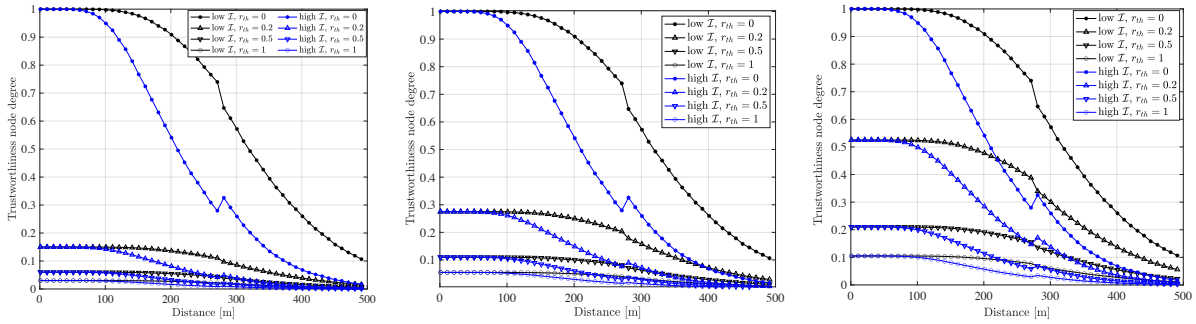
A similar trend is observed in case of Rural scenario, as reported in Fig. 3, still for different interference levels and reputation thresholds. In this case, we observe a sparse behavior of the trustworthiness node degree, which reaches low values for longer distances. Specifically, in Fig. 3(*a*) a trustworthiness degree of ≈ 0.6 is achieved for 300 m in case of low interference and for $r_{th} = 0$, while at the same distance for $r_{th} = 0.2$ the trustworthiness degree is reduced to 0.1. Better trends are observed for high values of friendship degree, as shown in Fig. 3(*b*) and (*c*). In the latter case, the trustworthiness degree reaches ≈ 0.5 for a distance of 100 m and $r_{th} = 0.2$, while for the same parameters but assuming a lower friendship degree of $\delta_{f,(i,j)} = 10$ the trustworthiness degree does not overcome 0.3.

The dependence of the trustworthiness degree from the reputation threshold r_{th} is depicted in Fig. 4 and Fig. 5, for UrbanMacro and Rural scenarios, respectively. We observe a decreasing trend of the trustworthiness node degree for increasing reputation threshold, occurring in case of low and high interference level and fixed values of inter-vehicle distance. Also in this case, high interference causes a reduction of trustworthiness degree, given a distance, as well as increased values are achieved for increasing friendship degree. Specifically, assuming a high interference level, a fixed distance of



(*a*) (*b*) (*c*)

Fig. 2. Comparison of the trustworthiness degree versus the distance in case of UrbanMacro scenario and for different values of friendship degree *i.e.*, (*a*) $\delta_f = 5$, (*b*) $\delta_f = 10$, and (*c*) $\delta_f = 20$.



(*a*) (*b*) (*c*)

Fig. 3. Comparison of the trustworthiness degree versus the distance in case of Rural scenario and for different values of friendship degree *i.e.*, (*a*) $\delta_f = 5$, (*b*) $\delta_f = 10$, and (*c*) $\delta_f = 20$.

$d = 40$ m and a reputation threshold of 0.4, the trustworthiness degree is limited to 0.1 and 0.2 for $\delta_{f,(i,j)} = 5$ and $\delta_{f,(i,j)} = 10$, respectively. On the other hand, for the same reputation threshold, distance, and interference level, it is possible to reach a trustworthiness degree of ≈ 0.3 for $\delta_{f,(i,j)} = 20$. We can evince that the friendship degree, which is responsible of the reputation degree, affects the trustworthiness node degree by increasing the trend in case of higher values.

Moving from UMa scenario to Rural, it is possible to observe how longer distances may be reached with positive values of trustworthiness degree. This behavior is depicted in Fig. 5 where the inter-vehicle distance reaches 400 m still providing positive values of trustworthiness. As compared to UMa scenario in Fig. 4, we notice that for a reputation threshold of 0.4 the trustworthiness degree is 0.15 for $d = 200$ m, while a close value of 0.18 is achieved still for $r_{th} = 0.4$ but for $d = 90$ m in case of UMa scenario. Finally, similar considerations apply to the results achievable in UMi scenario, which are not reported in this paper for room constraint.

V. Conclusions

In this work, we have investigated the trustworthiness concept in the context of mobile wireless networks, by accounting of physical layer features. Indeed, if from one side trustworthiness is recognized as a key concept to handling in a more robust way the interactions between different nodes, some important open challenges are persisting, hindering the development of trust solutions in real wireless systems. In this work, we have analyzed the impact of physical features and channel conditions impact on the system, in order to make the analysis closer to real-world scenarios. In particular, different levels of interference have been considered and their impact on the trustworthiness has been evaluated. This concept is also paramount, when the re-integration of a node whose trustworthiness has been lowered is considered. Indeed, when the a communication system is characterized with high interference, nodes can be unfairly lowered in terms of trust, by considering node degree based on the number of interactions and the aptitude to sending data to other nodes.

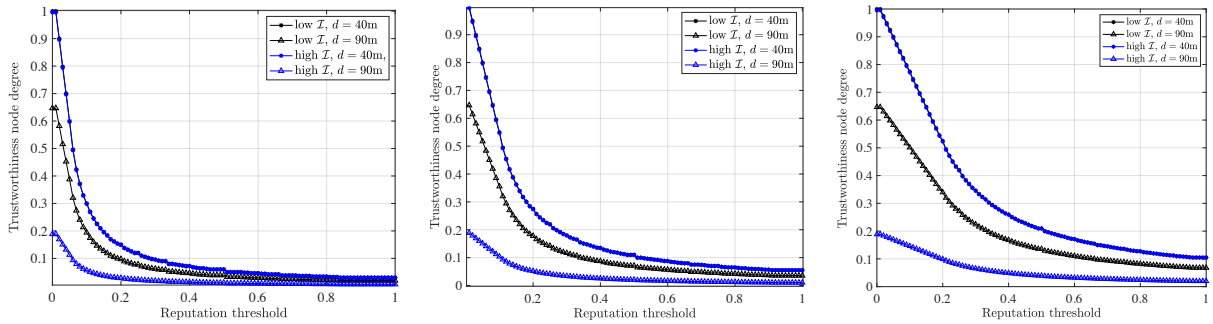


Fig. 4. Comparison of the trustworthiness degree versus the reputation threshold in case of UrbanMacro scenario and for different values of friendship degree *i.e.*, (*a*) $\delta_f = 5$, (*b*) $\delta_f = 10$, and (*c*) $\delta_f = 20$.

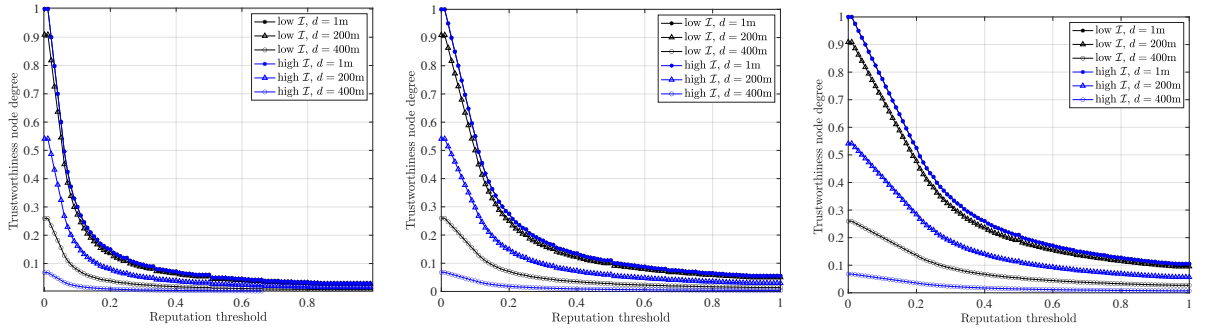


Fig. 5. Comparison of the trustworthiness degree versus the reputation threshold in case of Rural scenario and for different values of friendship degree *i.e.*, (*a*) $\delta_f = 5$, (*b*) $\delta_f = 10$, and (*c*) $\delta_f = 20$.

ACKNOWLEDGMENT

(Part of) this work was funded by the French National Research Agency (ANR-22-PEFT-0007) as part of France 2030 and the NF-FITNESS project.

REFERENCES

[1] E. Lee, E.-K. Lee, M. Gerla, and S. Y. Oh, "Vehicular cloud networking: architecture and design principles," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 148–155, 2014.

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

[3] B. Zhang, R. Tian, and C. Li, "Content dissemination and routing for vehicular social networks: A networking perspective," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 118–126, 2020.

[4] F. Jameel, S. Wyne, M. A. Javed, and S. Zeadally, "Interference-aided vehicular networks: Future research opportunities and challenges," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 36–42, 2018.

[5] Puñal, C. Pereira, A. Aguiar, and J. Gross, "Experimental characterization and modeling of rf jamming attacks on vanets," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 2, pp. 524–540, 2015.

[6] N. Haron *et al.*, "Data trustworthiness in internet of things: A taxonomy and future directions," in *2017 IEEE Conference on Big Data and Analytics (ICBDA)*, 2017, pp. 25–30.

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

[8] C. Boudagdigue *et al.*, "Trust management in industrial internet of things," *IEEE Trans. on Information Forensics and Security*, vol. 15, pp. 3667–3682, 2020.

[9] N. Thomas and S. Patil, "Trustworthiness of Data in IoT Crowd Sensing Environments," in *2022 Intl. Conf. on Futuristic Technologies*, 2022, pp. 1–5.

[10] M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: A Trustworthy Forensic Investigation Framework for the Internet of Vehicles (IoV)," in *2017 IEEE Intl. Congress on Internet of Things*, 2017, pp. 25–32.

[11] J. Wang *et al.*, "A Survey on Trust Models in Heterogeneous Networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2127–2162, 2022.

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

[13] A. Bhargava, S. Verma, B. K. Chaurasia, and G. S. Tomar, "Computational trust model for Internet of Vehicles," in *2017 Conf. on Information and Communication Technology*, 2017.

[14] J. Shen *et al.*, "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.

[15] A. M. Vegni, C. Leoni, V. Loscrí, and A. Benslimane, "A reputation-based trustworthiness concept for wireless networking in vehicular social networks," *IEEE Communications Magazine*, pp. 1–7, 2023.