IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON EMERGING TECHNOLOGIES ON VEHICLE TO EVERYTHING (V2X)

Received December 15, 2018, accepted January 3, 2019, date of publication January 17, 2019, date of current version February 12, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2893262

Decentralized Trust Evaluation in Vehicular Internet of Things

SIRI GULENG[1], CELIMUGE WU[2], (Senior Member, IEEE), XIANFU CHEN[3], (Member, IEEE), XIAOYAN WANG[4], (Member, IEEE), TSUTOMU YOSHINAGA[2], (Member, IEEE), AND YUSHENG JI[5], (Senior Member, IEEE)

[1]Hohhot Minzu College, Hohhot 010051, China
[2]Graduate School of Informatics and Engineering, The University of Electro-Communications, Tokyo 182-8585, Japan
[3]VTT Technical Research Centre of Finland, FI-90571 Oulu, Finland
[4]Graduate School of Science and Engineering, Ibaraki University, Hitachi 316-8511, Japan
[5]Information Systems Architecture Research Division, National Institute of Informatics, Tokyo 101-8430, Japan

Corresponding author: Celimuge Wu (clmg@is.uec.ac.jp)

This work was supported in part by the Inner Mongolia Science and Technology Major Project, in part by the National Institute of Informatics, Japan, through the Open Collaborative Research Program under Grant FY2018, in part by the Telecommunications Advanced Foundation, and in part by JSPS KAKENHI under Grant 16H02817, Grant 16K00121, and Grant 17K12670.

ABSTRACT Trust management in a decentralized vehicular network, such as vehicular ad hoc network, is particularly challenging due to the lack of centralized communication infrastructure and a fast varying feature of the vehicular environment. In this paper, we propose a decentralized trust management scheme for vehicular networks. The proposed scheme uses a fuzzy logic-based trust calculation approach to evaluate the direct trust where trustee nodes are located within the transmission range of a trustor node. A reinforcement learning-based approach is also employed to estimate the indirect trust where the behaviors of trustee cannot be observed directly. The extensive simulations are conducted to show the advantage of the proposed scheme over other baseline approaches.

INDEX TERMS Vehicular ad hoc networks, trust management, fuzzy logic, Q-learning.

I. INTRODUCTION

In recent years, Internet of Things (IoT) technologies have attracted great interests. Earlier types of IoT applications mainly focus on the sensing and collection of physical world information to the cyber world. In contrast, Cyber-Physical Systems (CPS) is used to control the physical world entities from the cyber world. Emerging IoT and CPS applications in various fields, including smart city, smart home, e-healthcare, smart transportation, and so on, critically require a trust management system that is able to check the trustworthiness of a node. Especially for the mission-critical and performance-sensitive applications such as autonomous driving, the design of a more intelligent and powerful trust management architecture [1]–[4] is in an urgent need.

In this paper, we study the trust management architecture for vehicular ad hoc networks (VANET) [5], [6]. VANET technology is one of main components supporting autonomous driving and intelligent transportation systems. However, due to some specific features of VANETs, the trust management in VANETs is a very challenging research issue. First, IoT devices (including vehicles) can hardly have good access to the cloud, which incurs a problem in the trust management as the trust evaluation should be conducted in a distributed way by using decentralized communications between devices. Since there is no centralized controller that can observe the behavior of all nodes, it is important to design a multi-agent trust management approach where multiple agents communicate with each other to evaluate an event correctly. Second, the dynamic topology of VANETs requires that the trust management system should be capable of handling complex situations. Since VANETs involve multiple types of devices and different types of communications, the environment could frequently change with time, which requires more intelligent communication architecture with dynamic adaptation and self-evolving capability.

Although there have been many studies related to networking protocols for VANETs, the trust management problem is an under-explored research topic. Existing studies do not sufficiently address the following issues. First, a non-cooperative behavior of not forwarding a packet could be because the node does not receive the packet at all. Second, a node generates a fake message could be because unintentional

reasons such as naive forwarding of packets from others. Third, some generated report messages could be lost at some nodes due to lossy wireless channels. Therefore, the trust management scheme should consider all these lossy and uncertain situations.

In this paper, we propose a decentralized trust management scheme for VANETs. In the proposed scheme, each node conducts a direct trust evaluation about each one-hop neighbor based on its behavior and other neighbors' reports. Indirect trust evaluation (trust evaluation about a node that is not directly reachable through one-hop wireless communications) is conducted for each non-one-hop-neighbor considering the reports from multiple one-hop neighbors, which is possible to handle complex situations by efficiently integrating knowledge from multiple nodes. The main contributions of this paper are as follows.

- We propose a fuzzy logic-based approach to evaluate the trust of one-hop neighbors. The proposed approach takes into account three different factors, namely, cooperativeness, honestness, and responsibility factors. Since the fuzzy logic-based approach is able to handle the complex and uncertain behavior of vehicles, it is suitable for dynamic and lossy vehicular networks.
- We propose a Q-learning approach to evaluate indirect trust of nodes that are not directly connected to a trustor node. An evaluation about a non-neighbor-node is conducted by averaging the evaluation reports from multiple nodes, which makes the evaluation result being robust to packet losses and detection errors at some nodes.
- We launch computer simulations to evaluate the proposed scheme in terms of both the malicious node detection efficiency and the corresponding effect on the communication performance.

The remainder of the paper is organized as follows. Section II provides a quick overview of existing studies. In section III, we describe the proposed scheme in details. Simulation results are presented in section IV. Finally, we draw our conclusions and future work in section V. The terms ''vehicle'' and ''node'' are used interchangeably throughout the paper.

II. RELATED WORK

We classify the existing works into two main categories, namely, the trust evaluation, and the trust management between certain communication pairs. The former one focuses on the trust computation and evaluation for a certain node. The latter one discusses how to ensure the trustworthiness of communications between a pair of nodes. This paper aims to propose an efficient trust evaluation scheme which is the basis for providing the trustworthiness.

A. TRUST COMPUTATION AND EVALUATION

The recent surveys on trust computation and evaluation can be found in [7] and [8]. Li and Song [9] have proposed an attack-resistant trust management scheme for VANETs. While the trust evaluation is conducted based on the data collected from multiple vehicles, the inaccurateness and incompleteness of the data due to the lossy wireless channel are not addressed in [9]. The indirect trust evaluation is not discussed sufficiently as well. Weng *et al.* [10] have proposed a credibility model that is used to mitigate the negative effects of wrong testimonies. The usefulness of a testimony is evaluated based on the past behaviors of the same node. However, uncertainties of the wireless channel are not addressed, which could deteriorate the performance of trust evaluation in a dynamic and lossy environment, such as VANETs.

Ahmad *et al.* [11] have proposed a trust computation framework that defines different levels of trust values for different types of vehicles, namely, higher authority (HA) vehicles (such as ambulances), public transport vehicles, professional, and ordinary cars. However, the problem of how to differentiate among different ordinary cars is not discussed adequately. Yang *et al.* [12] have proposed a trust management approach where the blockchain technology is used to store the trust values of vehicles. However, since the RSUs are used to calculate the offset of trust values for every involved vehicle using specific methods, the approach does not work for a totally distributed scenarios where RSUs do not exist. Huang *et al.* [13] have proposed a reputation management system based on vehicular edge computing technology where edge servers are adopted to execute local reputation management tasks for vehicles. However, similar to [12], RSUs or base stations are required to transmit vehicle data to edge servers.

A cloud-based trust management framework for vehicular social networks has been proposed in [14]. Depending on the involvement of cloud, [14] cannot provide a trust management solution for decentralized vehicular networks. Zhu *et al.* [15] have designed an interactive filtering truth discovery algorithm to judge a node is whether malicious node or not. However, [15] is a deterministic approach. Rostamzadeh *et al.* [16] have proposed a trust-based information dissemination framework based on an assumption that some areas of a city are safer than others by using better facilities. Relying on some pre-installed infrastructures to conduct trust management, [16] is not a totally decentralized approach, especially for the direct trust evaluation.

B. TRUST MANAGEMENT FOR A PAIR OF COMMUNICATION NODES

Zhong *et al.* [17] have proposed a conditional privacy-preserving authentication scheme that reduces the communication overhead by using the registration list instead of the revocation list. Li *et al.* [18] have proposed a physical layer key extraction method that uses the received signal strength to generate secret keys. Liu *et al.* [19] have proposed an authentication scheme to enhance security and privacy for V2V communications in intelligent transportation systems by exploiting the advantage of bilinear pairing to compute encryption key without additional key management. Zhang *et al.* [20] have proposed a vehicular authentication protocol where a vehicle can verify multiple messages

simultaneously and compress their signatures into a single one, which can greatly reduce the storage space. Rabieh *et al.* [21] have proposed two variants for VANETs, namely, elliptic curve cryptography point-addition-based route sharing scheme and homomorphic encryption-based route sharing scheme. Rajput *et al.* [22] have proposed a hierarchical pseudonymous authentication protocol with conditional privacy preservation, which employs two-level hierarchy for the pseudonyms with different life times. Vijayakumar *et al.* [23] have presented a dual authentication scheme to prevent malicious vehicles entering into the VANET systems, and proposed a dual key management technique to distribute group keys securely. Aiming at preserving security and privacy between a communication pair, these studies do not discuss whether a node should be trusted.

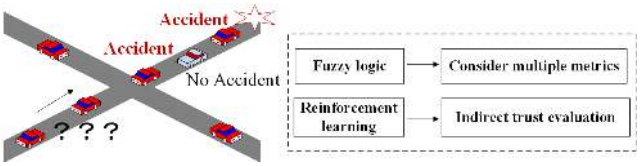

FIGURE 1. Multi-agent trust evaluation for decentralized vehicular IoT.

III. PROPOSED SCHEME

A. TRUST MANAGEMENT IN DECENTRALIZED VEHICULAR IOT

Due to the lack of centralized controller, the trust management in a decentralized vehicular IoT environment is particularly challenging. As shown in Fig.1, a vehicle could receive ''accident'' information from some nodes while receiving ''no accident'' information from other nodes that are dishonest. The trust management should include both the trust about a message and the trust about a node. There have been some studies discussing about the trust management problem in vehicular ad hoc networks. However, the indirect trust management is not seriously discussed in the literature. Since each node only can observe the events happening in its sensing range directly, the events that are occurring outside the sensing range should be evaluated based on the information received from other nodes. In a vehicular network, each vehicle's sensing range is limited due to buildings and other vehicles (for example, the radar sensor and camera sensor cannot detect a non-line-of-sight position).

There exist three main challenges in the design of trust evaluation. First, the evaluation of direct trust should take into account multiple factors such as the position information, trust of vehicles in vicinity, the relationship between vehicles, and the history of node behaviors. Second, the decentralized topology makes the evaluation of indirect trust particularly difficult. Third, the vehicle mobility requires that the trust evaluation should be conducted in a fast way.

B. OVERVIEW OF THE PROPOSED SCHEME

We propose a multi-agent trust evaluation approach where the direct trust is evaluated by considering different factors with a fuzzy logic algorithm. The indirect trust evaluation is conducted by using a reinforcement learning approach that discounts a trust according to the number of relays. The direct trust evaluation is conducted by taking into account the behaviors of nodes in three different aspects, namely, cooperativeness, honestness, and responsibility factors. These three factors are jointly considered by a fuzzy logic-based algorithm. Each node also updates its trust evaluation value for none-neighbor nodes using a Q-learning algorithm.

Each node (vehicle) has a unique ID. The source node of a packet (originator of the packet) will add its ID to the data packets that are generated by it. The ID will be encrypted by the private key of the node, and a receiver node can check the ID by decrypting the ID with the public key of the source node. In this way, each node in the transmission range is possible to check the originator node information of a packet. Each node attaches its position information and observed information in the hello messages. The observed information includes the accident information, traffic alert information, and the packet forwarding information as shown in Table 1.

TABLE 1. Information exchanged among neighbors.

Position information
Accident information, traffic alert information, etc.
Packet forwarding request: {destination, next hop, number of packets}
Packet forwarding info: {destination, next hop, number of packets}

C. FUZZY LOGIC-BASED DIRECT TRUST CALCULATION

The direct trust evaluation process consists of three steps. First, the cooperativeness factor, the honestness factor, and the responsibility factor are evaluated for each one-hop neighbor. Next, these factors are converted to fuzzy values, and then calculated by predefined rules to get the final fuzzy value. Last, the fuzzy value is converted to a numerical value (i.e., the competency value) based on fuzzy output membership function. The final numerical value shows the trustworthiness level of the corresponding trustee node.

1) FIRST STEP – CALCULATION OF THREE FACTORS

a: COOPERATIVENESS FACTOR (CF)

CF is calculated by

$$CF(m) = \begin{cases} \dfrac{N_F(m)}{N_O}, & \text{if } N_F(m) < N_O \ \& \ N_O \neq 0 \\ 1, & \text{otherwise} \end{cases} \quad (1)$$

where $N_F(m)$ is the number of packets forwarded by m, and N_O is the average number of packets observed at neighbors. N_O is calculated by collecting forwarding status report from one-hop neighbors. The CF factor shows how much the trustee node conducted the forwarding jobs allocated to it. A larger value means that the trustee node is more cooperative. By using this factor, the selfish behavior of trustee nodes can be considered in the trust evaluation. The calculation of Eq.(1) is conducted for each 100-second time period, and then

updated based on a weighted exponential moving average as

$$CF_i(m) \leftarrow (1-\alpha) \times CF_{i-1}(m) + \alpha \times CF_i(m), \quad (2)$$

where $CF_i(m)$ is the current value and $CF_{i-1}(m)$ is the previous value. Smoothing factor α is set to 0.7. Note that the length of time period used for the calculation can be tuned according to the application requirements. The weighted exponential moving average is used to smooth the evaluation value, making it more robust to small errors.

b: HONESTNESS FACTOR (HF)

HF is calculated by

$$HF(m) = \begin{cases} \dfrac{N_H(m)}{N_S(m)}, & \text{if } N_H(m) < N_S(m) \ \& \ N_S(m) \neq 0 \\ 1, & \text{otherwise} \end{cases} \quad (3)$$

where $N_H(m)$ is the number of honest packets sent by m, and $N_S(m)$ is the number of packets sent by m. The HF factor shows how many percent of the packets sent by the trustee node is true. If a trustee node lies about the events happening in vicinity, the corresponding HF becomes lower. In contrast, if the trustee node is honest with its neighbors about its observation, the node gets a higher HF. HF is updated as

$$HF_i(m) \leftarrow (1-\alpha) \times HF_{i-1}(m) + \alpha \times HF_i(m). \quad (4)$$

c: RESPONSIBILITY FACTOR (RF)

RF is calculated by

$$RF(m) = \begin{cases} \dfrac{N_R(m)}{N_A}, & \text{if } N_R(m) < N_A \ \& \ N_A \neq 0 \\ 1, & \text{otherwise} \end{cases} \quad (5)$$

where $N_R(m)$ is the number of packets that are included in the status report of m, and N_A is the average number of packets that are reported by other neighbors. The RF is used to show how much percent of the events that detected by the trustee node are reported by the trustee node. This factor is different from CF in that RF is more focused on showing the jobs done by the trustee node regarding event detection while CF is used to show the packet forwarding behavior. In order to detect an event correctly, we have to collect enough reports from different nodes. This is why we use RF in the trust evaluation. RF is updated as

$$RF_i(m) \leftarrow (1-\alpha) \times RF_{i-1}(m) + \alpha \times RF_i(m). \quad (6)$$

2) SECOND STEP – FUZZIFICATION AND FUZZY RULES

The fuzzy membership functions for CF, HF and RF are defined as shown in Fig. 2, Fig. 3 and Fig. 4, respectively.

Fuzzy rules are defined as shown in Table 2 where Rule1 is expressed as follows.

IF *Cooperativeness* is Good, *Honestness* is Good, and *Responsibility* is Good **THEN** *Rank* is Perfect.

Based on Table 2, the fuzzy value for a trustee node can be calculated. The calculation approach is the same as [24]. We use the Min-Max method in the case that multiple rules apply at the same time.

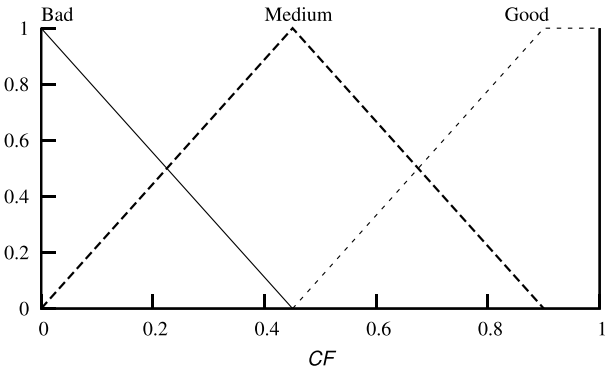

FIGURE 2. Fuzzy membership function for *CF*.

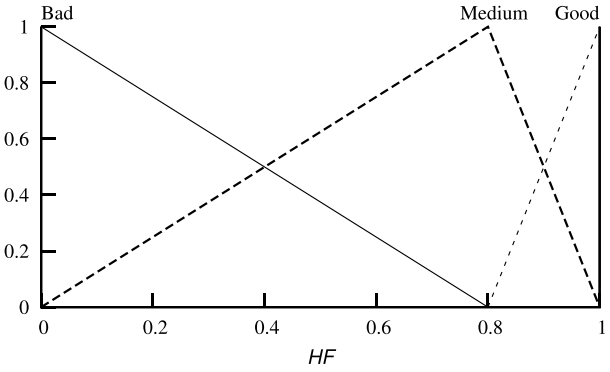

FIGURE 3. Fuzzy membership function for *HF*.

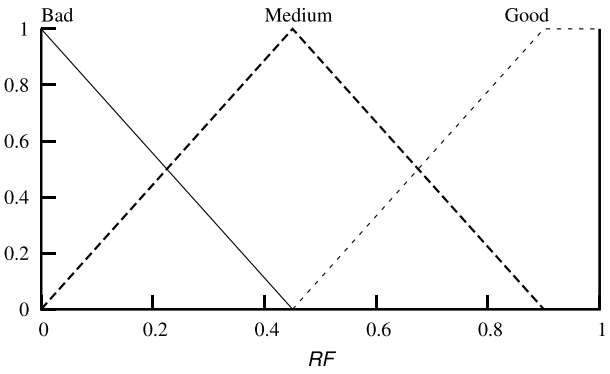

FIGURE 4. Fuzzy membership function for *RF*.

3) LAST STEP – DEFUZZIFICATION

Fig. 5 shows the output membership function that is used to defuzzify the result in order to get the trust evaluation value of the node. By comparing the competency values, we can know which node is the most trustable.

D. INDIRECT TRUST CALCULATION BASED ON Q-LEARNING

Each node only can observe the events occurring in the neighborhood. For a trust evaluation about a trustee node beyond the transmission range, the node has to conduct a judgement based on other nodes' knowledge. Here we use a Q-learning

TABLE 2. Rule base.

	CF	HF	RF	Rank
Rule1	Good	Good	Good	Perfect
Rule2	Good	Good	Medium	Good
Rule3	Good	Good	Bad	Unpreferable
Rule4	Good	Medium	Good	Good
Rule5	Good	Medium	Medium	Acceptable
Rule6	Good	Medium	Bad	Bad
Rule7	Good	Bad	Good	Unpreferable
Rule8	Good	Bad	Medium	Bad
Rule9	Good	Bad	Bad	VeryBad
Rule10	Medium	Good	Good	Good
Rule11	Medium	Good	Medium	Acceptable
Rule12	Medium	Good	Bad	Bad
Rule13	Medium	Medium	Good	Acceptable
Rule14	Medium	Medium	Medium	Unpreferable
Rule15	Medium	Medium	Bad	Bad
Rule16	Medium	Bad	Good	Bad
Rule17	Medium	Bad	Medium	Bad
Rule18	Medium	Bad	Bad	VeryBad
Rule19	Bad	Good	Good	Unpreferable
Rule20	Bad	Good	Medium	Bad
Rule21	Bad	Good	Bad	VeryBad
Rule22	Bad	Medium	Good	Bad
Rule23	Bad	Medium	Medium	Bad
Rule24	Bad	Medium	Bad	VeryBad
Rule25	Bad	Bad	Good	Bad
Rule26	Bad	Bad	Medium	VeryBad
Rule27	Bad	Bad	Bad	VeryBad

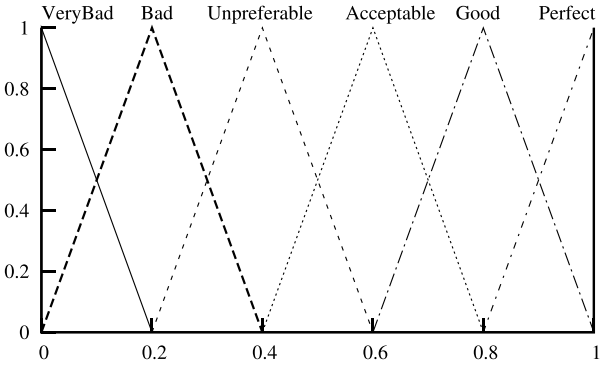

FIGURE 5. Output membership function.

algorithm to conduct indirect trust evaluation by discounting the trust value with the hopping of trust value and the trust values of the forwarders.

1) Q-LEARNING MODEL

In the proposed protocol, a Q-learning algorithm is used to evaluate the trust value of a node that is not within the transmission range. The following Q-learning model is defined. The environment is the entire network. The network nodes are the learning agents, and they learn the environment by exchanging hello messages with each other. Each node is a state. A possible action at each node is the selection of a neighbor's knowledge in the trust evaluation. Each node calculates the trust value for a non-neighbor node based on its neighbors' evaluations. Each node maintains a Q-Table where each Q-value $[Q(d, m)]$ shows the trust value for node d based on the information received from m.

2) UPDATE OF Q-VALUES

Each node has to maintain a Q-value for each pair of a trustee node (both neighbor nodes and non-neighbor nodes) and a neighbor node. Upon reception of each hello message, the Q-Table is updated. Q-values are attached to the hello messages and broadcasted by all nodes. The initial value for each Q-value is 0. After reception of a hello message from node m, node l updates the corresponding Q-value to node d as

$$\begin{aligned} Q_l(d,m) \leftarrow\ & \hat{\alpha} \times Q_l(d,m) \\ & \times \left\{ \hat{R} + \gamma \times \text{avg}_{y \in NB_m} Q_m(d,y) \right\} \\ & + (1-\hat{\alpha}) \times Q_l(d,m). \end{aligned} \tag{7}$$

where $Q_l(d, m)$ is the trust evaluation value about node m (calculated at node l). NB_m denotes the one-hop neighbor set of node m.

The learning rate $(\hat{\alpha})$ is 0.7, and the discount factor (γ) is 0.9. $\text{avg}_{y \in NB_m} Q_m(d, y)$ is the average Q-value of m to node d. The reward $\hat{R}$ is calculated as

$$\hat{R} = \begin{cases} DT, & \text{if } l \in NB_d \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

where DT is the direct trust value for node d observed at node l as calculated by the fuzzy logic-based trust evaluation. NB_d denotes the one-hop neighbor set of node d. If node l is a neighbor of node d, the reward is DT and otherwise 0. Each Q-value is an evaluation value for each pair of state and action. Upon reception of a hello message, each agent updates the corresponding Q-value as shown in Eq.(7).

The reward is discounted by two elements, specifically, the number of hops from the trustee node (d), and the trust value of each node contributed to this evaluation (all the nodes forwarding the trust value from the node d to the current node). The consideration of hop count ensures that the evaluation intends to count more the directly observed trust. Each Q-value is a representation of the trust value of node d based on the information received from node m. Note that node m could receive different trust values from different neighbors, where the final trust value will be the average of these values $[\text{avg}_{y \in NB_m} Q_m(d, y)]$. We use average value here in order to reduce the effect of malicious nodes. This does not affect the convergence of the proposed scheme because all the possible actions could be visited through the broadcast of hello messages at each node, and the algorithm could finally converge to a synthetic evaluation of multi-hop trust values. By discounting a trust value with the trust forwarding, the protocol is able to evaluate an indirect trust, achieving a fair evaluation for a node that is not directly observable.

IV. SIMULATION RESULTS

We used ns-2.34 [25] to conduct simulations in freeway scenarios (see Table 3). We used a freeway which had two lanes

TABLE 3. Simulation environment.

Topology	2000m, 4lanes
Number of nodes	200
Maximum velocity	100 km/h
Mobility generation	Ref. [26]
MAC	IEEE 802.11p MAC (27 Mbps)
Propagation model	Nakagami model
Simulation time	1500 s

TABLE 4. Parameters of Nakagami model.

gamma0_	gamma1_	gamma2_	d0_gamma_	d1_gamma_
1.9	3.8	3.8	200	500
m0_	m1_	m2_	d0_m_	d1_m_
1.5	0.75	0.75	80	200

in each direction [26]. The distance between any two adjacent lanes was 5m. Nakagami propagation model was used to simulate channel fading [27]. The parameters of Nakagami Model are shown in Table 4, where parameter names are the variable names in ns-2.34. Based on parameters given in [27], we set the average transmission range for IEEE 802.11p communications as 250m. The corresponding packet delivery ratio with the distance is shown in Fig.6.

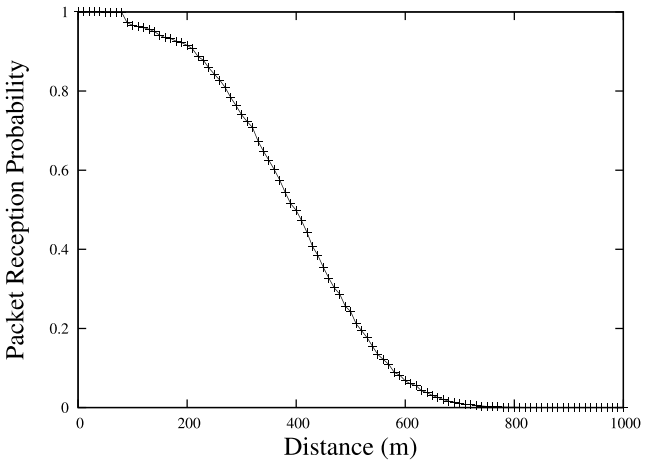

FIGURE 6. Packet reception probability for various distances.

The proposed protocol was compared with "w/o Trust" (without trust), and "Deterministic trust". "w/o Trust" denotes the approach without trust management. In "Deterministic trust", a trust value is evaluated deterministically based on the direct or indirect observation, where "deterministic" means that if a node is evaluated as a malicious node and then will be considered as a malicious node forever. In the simulation, malicious nodes used "Bad Mouth Attack" with 0.3 probability and dropping packet with 0.3 probability. In the following simulation results, the error bars indicate the 95% confidence intervals.

A. PRECISION

Fig. 7 shows the precision for various numbers of malicious nodes. In order to clearly show the evaluation result, in this figure, all the trustee nodes are neighbors (only direct

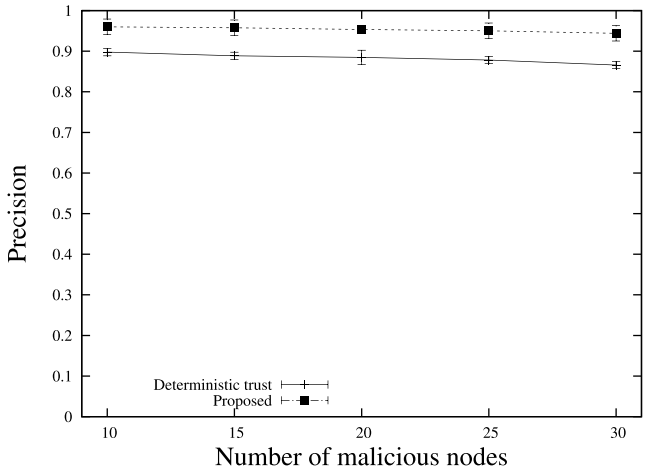

FIGURE 7. Precision for various numbers of malicious nodes (direct trust).

trust is evaluated). Precision is calculated as

$$\text{Precision} = \frac{\text{Number of malicious nodes correctly judged}}{\text{Number of malicious nodes detected}}. \quad (9)$$

It is easy to observe that "Deterministic trust" is unable to achieve a high precision. Due to the vehicle mobility and lossy vehicular communication channel, "Deterministic trust" could make wrong evaluations, such as detecting a packet loss as a non-cooperative behavior. This explains the advantage of the fuzzy logic-based approach that conducts a joint evaluation based on the cooperativeness factor, the honestness factor, and the responsibility factor.

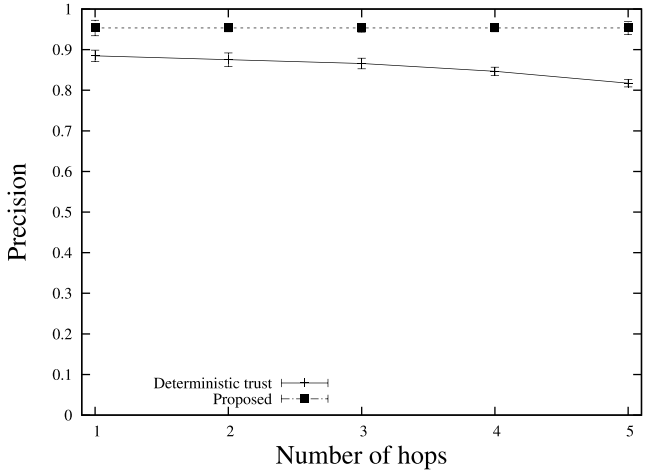

FIGURE 8. Precision for various numbers of hops (in case of 20 malicious nodes).

Fig. 8 shows the precision for various numbers of hops when the number of malicious nodes is 20. As shown in Fig. 8, with the number of hops increases, the precision of "Deterministic trust" drops drastically due to the deterministic decision making which is incapable of handling fast varying vehicular environment. Due to the fuzzy logic-based

direct trust evaluation and reinforcement learning-based indirect trust calculation, the proposed scheme is able to provide a high precision for various numbers of hops.

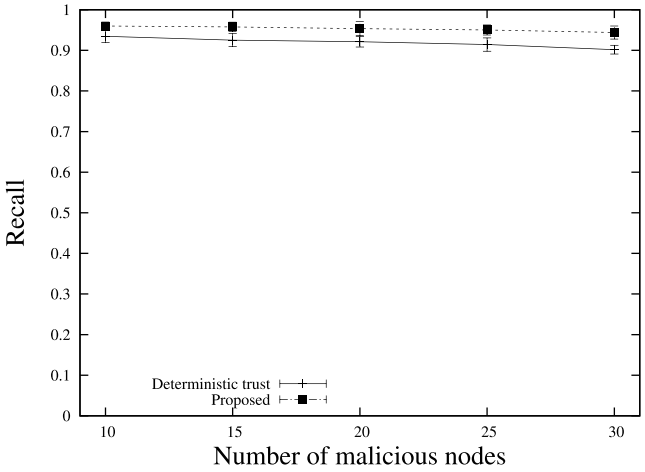

FIGURE 9. Recall for various numbers of malicious nodes (direct trust).

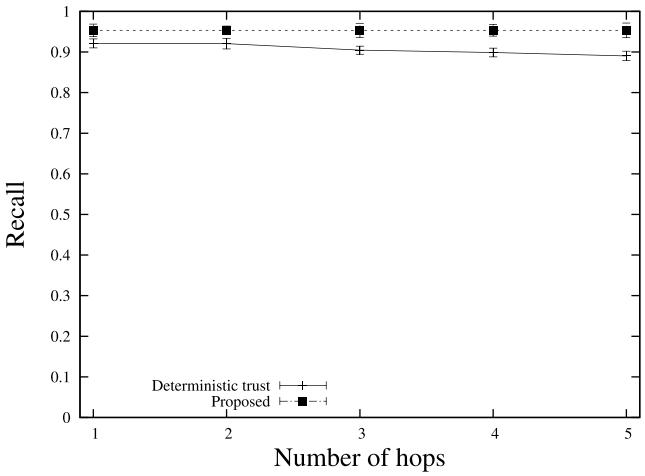

FIGURE 10. Recall for various numbers of hops (in case of 20 malicious nodes).

Fig. 9 and Fig. 10 show the recall rates for various numbers of malicious nodes and various numbers of hops, respectively. Here, recall is calculated as

$$\text{Recall} = \frac{\text{Number of malicious nodes correctly judged}}{\text{Number of malicious nodes}}. \tag{10}$$

"Deterministic trust" cannot provide a satisfactory result because it is sensitive to packet losses which could result in that the information collected is inaccurate. The proposed scheme judges a node based on the evaluations from other nodes, which contributes to a better result. Especially when the number of hops is larger, the advantage of the proposed scheme becomes more significant. This is because the proposed protocol uses the average Q-value for the final evaluation, resulting in a better understanding about the nodes located outside the transmission range.

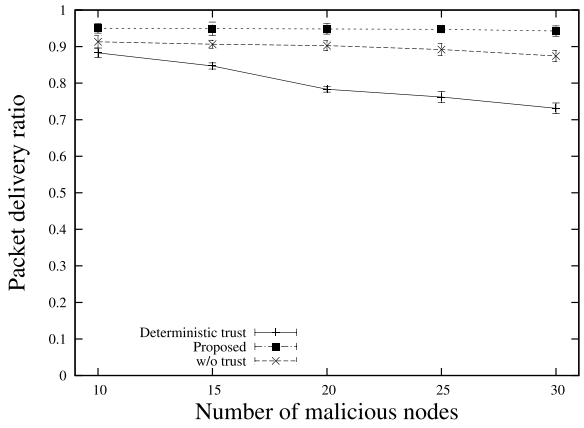

FIGURE 11. TCP throughput of unicast communications for various numbers of malicious nodes.

B. COMMUNICATION PERFORMANCE

We also evaluated the effect of the proposed scheme on networking performance under the existence of malicious nodes. Fig. 11 shows the packet delivery ratio of unicast communications for various numbers of malicious nodes. Other parameters were the same as the scenarios used in [28]. The performance difference between "Deterministic trust" and "w/o Trust" explains the importance of a trust management scheme in vehicular networks. Since the proposed scheme can achieve better precision and recall in detecting malicious nodes, it results in a significant improvement over "Deterministic trust" and "w/o Trust".

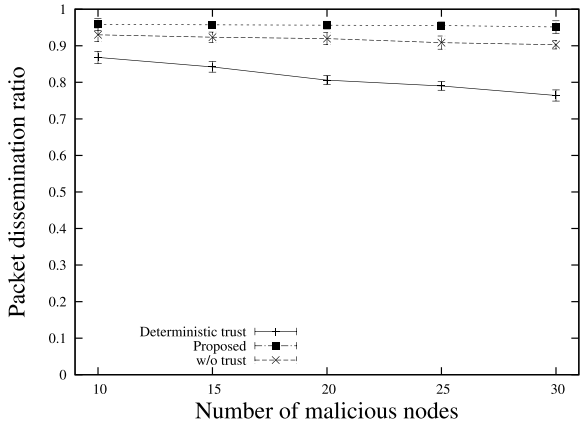

FIGURE 12. Packet dissemination ratio of broadcast communications for various numbers of malicious nodes.

Fig. 12 shows the packet dissemination in broadcast communications (packet altered is considered as undelivered). Other parameters were the same as the scenarios used in [24]. The proposed scheme is able to provide the best performance since it can efficiently avoid choosing a malicious node as a relay node.

V. CONCLUSIONS AND FUTURE WORK

We proposed a multi-agent trust management scheme for decentralized vehicular networks. The proposed scheme uses a fuzzy logic-based direct trust evaluation approach

to evaluate trusts about directly observable one-hop neighbor nodes by considering the dynamic topology and lossy communication channel of vehicular networks that could make the observation at each node imprecise. A reinforcement learning-based approach is used to calculate the indirect trust value of a node that is outside the directly observable region. In the indirect trust evaluation, the trust values of all nodes involved in the trust forwarding and the number of hops from the trustee nodes are considered in order to achieve an efficient and accurate trust evaluation. We used computer simulations to show the validity of trust evaluation approach, and the corresponding advantage on the networking performance by comparing with other baseline approaches.

In future work, we will consider combing this trust management scheme with VANET routing protocols. By using the trust value as a part of routing metric, the routing protocol can be more robust to selfish and adversary behaviors. The complexity of routing decision with multiple constraints, such as mobility, bandwidth, link quality, and trustworthiness, could open up many interesting research topics including trust-aware signaling and routing.

REFERENCES

[1] C. Burnett, T. J. Norman, K. Sycara, and N. Oren, "Supporting trust assessment and decision making in coalitions," *IEEE Intell. Syst.*, vol. 29, no. 4, pp. 18–24, Jul. 2014.

[2] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, 4th Quart., 2011.

[3] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1287–1309, 2nd Quart., 2016.

[4] C. Wu, Z. Liu, D. Zhang, T. Yoshinaga, and Y. Ji, "Spatial intelligence toward trustworthy vehicular IoT," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 22–27, Oct. 2018.

[5] C. Wu, T. Yoshinaga, Y. Ji, T. Murase, and Y. Zhang, "A reinforcement learning-based data storage scheme for vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6336–6348, Jul. 2017.

[6] J. Feng, Z. Liu, C. Wu, and Y. Ji, "AVE: Autonomous vehicular edge computing framework with ACO-based scheduling," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10660–10675, Dec. 2017.

[7] 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.

[8] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, to be published, doi: 10.1109/TITS.2018.2818888.

[9] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.

[10] J. Weng, Z. Shen, C. Miao, A. Goh, and C. Leung, "Credibility: How agents can handle unfair third-party testimonies in computational trust models," *IEEE Trans. Knowl. Data Eng.*, vol. 22, no. 9, pp. 1286–1298, Sep. 2010.

[11] F. Ahmad, V. N. L. Franqueira, and A. Adnane, "TEAM: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 28643–28660, 2018.

[12] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based Decentralized trust management in vehicular networks," *IEEE Internet Things J*, to be published, doi: 10.1109/JIOT.2018.2836144.

[13] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2018.

[14] X. Chen and L. Wang, "A cloud-based trust management framework for vehicular social networks," *IEEE Access*, vol. 5, pp. 2967–2980, 2017.

[15] L. Zhu, C. Zhang, C. Xu, and K. Sharif, "RTSense: Providing reliable trust-based crowdsensing services in CVCC," *IEEE Netw.*, vol. 32, no. 3, pp. 20–26, May/Jun. 2018.

[16] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, and V. C. M. Leung, "A context-aware trust-based information dissemination framework for vehicular networks," *IEEE Internet Things J.*, vol. 2, no. 2, pp. 121–132, Apr. 2015.

[17] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, "Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 2241–2250, 2018.

[18] X. Li, J. Liu, Q. Yao, and J. Ma, "Efficient and consistent key extraction based on received signal strength for vehicular ad hoc networks," *IEEE Access*, vol. 5, pp. 5281–5291, 2017.

[19] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2740–2749, Oct. 2017.

[20] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 516–526, Mar. 2017.

[21] K. Rabieh, M. M. E. A. Mahmoud, and M. Younis, "Privacy-preserving route reporting schemes for traffic management systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2703–2713, Mar. 2017.

[22] U. Rajput, F. Abbas, and H. Oh, "A hierarchical privacy preserving pseudonymous authentication protocol for VANET," *IEEE Access*, vol. 4, pp. 7770–7784, 2016.

[23] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 1015–1028, Apr. 2016.

[24] C. Wu, S. Ohzahata, and T. Kato, "VANET broadcast protocol based on fuzzy logic and lightweight retransmission mechanism," *IEICE Trans. Commun.*, vol. 95-B, no. 2, pp. 415–425, Feb. 2012.

[25] *The Network Simulator–ns-2*. Accessed: Sep. 23, 2018. [Online]. Available: http://www.isi.edu/nsnam/ns/

[26] F. Bai, N. Sadagopan, and A. Helmy, "Important: A framework to systematically analyze the impact of mobility on performance of routing protocols for adhoc networks," in *Proc. 22nd Annu. Joint Conf. IEEE Comput. Commun. Soc.*, Mar./Apr. 2003, pp. 825–835.

[27] A. Khan, S. Sadhu, and M. Yeleswarapu, "A comparative analysis of DSRC and 802.11 over vehicular Ad hoc networks," Dept. Comput. Sci., Univ. California, Santa Barbara, CA, USA, Tech. Rep., 2009, pp. 1–8.

[28] C. Wu, S. Ohzahata, and T. Kato, "Flexible, portable, and practicable solution for routing in VANETs: A fuzzy constraint Q-learning approach," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4251–4263, Nov. 2013.

SIRI GULENG is currently a Professor with the Hohhot Minzu College, China. His current research interests include computer systems and cybersecurity.

CELIMUGE WU received the M.E. degree from the Beijing Institute of Technology, China, in 2006, and the Ph.D. degree from The University of Electro-Communications, Japan, in 2010, where he is currently an Associate Professor with the Graduate School of Informatics and Engineering. His current research interests include vehicular ad hoc networks, sensor networks, intelligent transport systems, the Internet of Things, 5G, and mobile cloud computing. He is/has been a TPC Co-Chair of the Wireless Days 2019 and ICT-DM 2018 and a Track Co-Chair for many international conferences, including the ICCCN 2019 and the IEEE PIMRC 2016.

XIANFU CHEN received the Ph.D. degree in signal and information processing from the Department of Information Science and Electronic Engineering, Zhejiang University, Hangzhou, China, in 2012. He is currently a Senior Scientist with the VTT Technical Research Centre of Finland, Oulu, Finland. His research interests include various aspects of wireless communications and networking, with an emphasis on software-defined networking, green communications, centralized and decentralized resource allocation, dynamic spectrum access, and the application of artificial intelligence to wireless communications.

XIAOYAN WANG received the B.E. degree from Beihang University, China, and the M.E. and Ph.D. degrees from the University of Tsukuba, Japan. He was an Assistant Professor (by special appointment) with the National Institute of Informatics, Japan, from 2013 to 2016. He is currently an Assistant Professor with the Graduate School of Science and Engineering, Ibaraki University, Japan. His research interests include networking, wireless communications, cloud computing, big data, security, and privacy.

TSUTOMU YOSHINAGA received the B.E., M.E., and D.E. degrees from Utsunomiya University, in 1986, 1988, and 1997, respectively. From 1988 to 2000, he was a Research Associate with the Faculty of Engineering, Utsunomiya University. He was a Visiting Researcher with the Electro-Technical Laboratory, from 1997 to 1998. Since 2000, he has been with the Graduate School of Information Systems, The University of Electro-Communications, where he is currently a Professor. His research interests include computer architecture, interconnection networks, and network computing. He is a Fellow of IEICE and a member of ACM, the IEEE, and IPSJ.

YUSHENG JI received the B.E., M.E., and D.E. degrees in electrical engineering from The University of Tokyo. She joined the National Center for Science Information Systems, Japan, in 1990. She is currently a Professor with the National Institute of Informatics and with The Graduate University for Advanced Studies. Her research interests include network architecture, resource management, and quality of service provisioning in wired and wireless communication networks. She is/has been an Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, a Symposium Co-Chair of the IEEE GLOBECOM 2012 and the IEEE GLOBECOM 2014, and a Track Co-Chair of the IEEE VTC 2016-Fall and IEEE VTC 2017-Fall.