Bidding Price-based Transaction: Trust Establishment for Vehicular Fog Computing Service in Rural Area

Favian Dewanta, *Member, IEEE*
Kanazawa University
✉ *dewanta2308@stu.kanazawa-u.ac.jp*

Masahiro Mambo, *Member, IEEE*
Kanazawa University

***Abstract*—In the time of passing through rural area, vehicles sometimes need to deal with blank spots of wireless network (4G/5G/WiFi/others). As a result, vehicles are unable to access fog computing service based on road side unit (RSU) infrastructure. To deal with this situation, vehicles utilize other vehicles' huge computational resource during their travel. However, it is not easy to put trust on other unknown vehicles since it can lead to a serious consequence for both user and server of vehicular fog computing service. In this paper, we attempt to fill gaps on establishing a trusted vehicular fog computing environment by mean of bidding price-based transaction (BPT) method. Through this method, vehicles do not need to encounter any trusted third party to have fog computing transaction with other vehicles. Moreover, every malicious activity may cause actors to lose bidding and trust, and then victim will gain redeem point as the compensation for receiving loss in transaction. In the end, this novel method is effective in limiting the number of potential attacks by mean of bidding price and payoff.**

Keywords: Vehicular Network, Fog Computing, Trust Establishment

I. Introduction

Since the emergence of fog computing technology (the term of edge computing is also used to address the similar issue), there are a lot of applications that integrate fog computing technology into their native system. Vehicular network, also known as VANET, is one of the technologies that rapidly adapt fog computing into the system due to the need of real time and huge data processing [1].

In order to implement fog computing service (FCS), there are two basic approaches that can be adapted into VANET system: RSU- or 4G/5G-eNodeB-based FCS [2] [3] [4] and also vehicle-based FCS [5]. In terms of cost, the first one relies on high cost static infrastructure equipped with bigger computational resources on the road side as compared with the other one (vehicle-based FCS) that relies on low cost peer-to-peer and dynamic network topology change.

Due to the low traffic generation, sparse population, and energy sustainability issues, deploying network communication (tower) infrastructure in rural area is considered to be high cost investment and maintenance. Having those issues, some people in certain countries attempt to provide low cost network infrastructure by proposing wireless mesh network [6] or village wireless LAN [7]. In the same vein, we can presume that vehicle-based FCS is more appropriate to be applied in network-infrastructureless environment like rural area.

One may wonder whether vehicular FCS is possible in rural area due to low vehicular traffic and sparse village location. We argue it is feasible to realize it. As for illustration, we can consider the following situation. While running on rural area, vehicles may find some vehicles running in the same/opposite direction or parking in some places which own rich storage and computational resources [5]. Under these situations, those poor computational resource vehicles may have transaction with those rich computational resource vehicles by mean of vehicle-based FCS. Hereafter, we discuss the same network connectivity for vehicular fog computing service in rural area as already elaborated in [5].

As for applying fog computing service in dynamic network topology, there are some recent work that discuss about how to attract fog computing resource owners to contribute on supporting clients/users that need to offload certain heavy computation. In 2017, Liu et al. [8] discussed the mechanism to extend cloud computing service by mean of edge computing resource in several crowded areas, e.g. railway station, shopping mall, airport, etc. Their Stackelberg game approach was claimed to be effective to encourage edge computing in order to participate in giving computation offloading service to mobile users. In the same year, Yan et al. [9] proposed an algorithm to integrate sporadic resources in the local network as a dynamic resource pool in order to perform assigned task by the fog broker. Their simulation results showed that their crowd-funding algorithm method could reduce the service level agreement (SLA) violation rate and at the same time they could execute assigned tasks faster with respect to other two algorithms (MM and MBFD).

For establishing trusted vehicular network environment, several works also elaborate their method by mean of authentication, and also reputation/rating system. As for authentication, several ideas were proposed including estimating vehicle position based on signal strength distribution [10] and series of time-stamp [11]. There are also privacy-preserving anonymous ID authentication schemes by mean of RSU infrastructure [12], group signature [13], or certified session-key [14]. As for reputation and rating system, vehicles at first need to be recognized by RSU or a group of vehicles and then trust

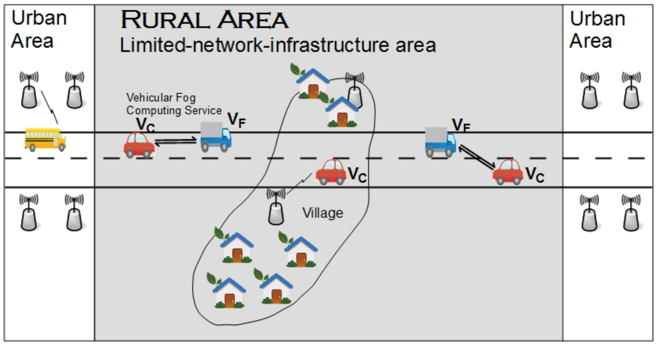

Fig. 1. System model of the proposed method

is usually established based on a majority vote from other entities, weighted trust parameter calculation, and also social network relationship as elaborated in [15] [16] [17].

However, it is difficult to implement the previous trust establishment schemes for vehicles since they mostly rely on trusted third party/RSU infrastructure while the vehicles may not always be trusted or honest. Furthermore, trusted third party and RSU infrastructure are not appropriate for rural area. In this paper, we offer trust establishment for vehicular fog computing in rural area based on certified bidding transaction. This method relies on price of bidding for guaranteeing transaction which can be redeemed later if one party violates the transaction by doing malicious activity. Eventually, through this method, it becomes more likely that vehicles in rural area can attain trusted fog computing service transaction.

II. System Model

A. Establishing Fog Computing Service in Rural Area

In this paper, rural area is defined as an area which is out of towns or cities. In some part of its area, it is inhabited by few number of people who are gathered in a village which may be equipped by network infrastructure. Thus, while passing the village, vehicle may use infrastructure-based fog computing service. Then, the rest of rural area is not inhabited and not equipped by network infrastructure. As a result, vehicle can only rely on ad-hoc/vehicular fog computing service by mean of vehicle-as-a-infrastructure of fog computing as given in Figure 1.

In the real implementation of vehicular fog computing service application, we cannot rely only on trust establishment scheme. Some coding schemes are also needed to guarantee data recovery and to minimize data loss in the chain of data migration among client vehicle V_C and fog computing vehicle V_F, which eventually arrives to fog node FN. These coding schemes are not new things for cloud or fog computing, as they have been implemented by mean of several software and also been discussed by Li et al. in [18]. However, this paper does not discuss those coding schemes issues nor how to enable them on this proposed scheme since trust establishment for vehicular fog computing service in rural area has not yet been discussed so much in comparison with those coding schemes.

Thus, our proposed method attempts to extend the service of infrastructure-based fog computing by utilizing other vehicle (V_F) resources which are huge enough to assist other vehicle (V_C) as depicted in Figure 1. This service is not intended to create standalone service system from infrastructure-based fog computing service system, nor to allow illegal and unauthenticated vehicle as the server or user of vehicular fog computing service. Instead, the vehicles are required to register to the infrastructure-based fog computing service provider to get certificate as the communication enabler for providing (V_F) or receiving (V_C) service. Thus, this system will protect both V_C and V_F from outsider or any unauthorized entities that may launch malicious actions.

Prior to pass through rural area, all vehicles should register themselves to infrastructure-based fog node (FN) in order to obtain new credentials to conduct ad hoc fog computing transaction on rural area. During registration process, vehicle deposits some amount of digital currency (C) for bidding and also specifying the compensation value of malicious activities conducted during ad hoc fog computing service transaction. After being accepted, FN then issues certified-public-credentials (CPC) $\langle ID, PK, C, Sign_P \rangle$ which mean identity of vehicle, public key, deposited digital currency for bidding on ad-hoc transaction, and signature from FN respectively. Along side with that CPC, FN also issues certified-secret-credential (CSC) $\langle SK, j, G, g, Sign_S \rangle$ which mean private key, juggling key, sub-group G and generator g derived from Z_p^* with prime order q, and also signature from FN.

Following the registration process, both V_F and V_C will enter the rural area and do some activities on the uncovered network area, either disaster recovery, rescue mission, agriculture, or just passing-through. When it comes to full occupied computation resource, vehicles need to find the closest fog computing service either to upload some important files so that system can write new files or to offload some heavy computations. In this kind of situation, vehicles (V_C) can utilize other vehicles resource (V_F) which are certified by the known FN. Then, the process of ad hoc fog computing service transaction is given in Figure 2 and the following description steps.

1) **Certificate exchange**. Both V_C and V_F will exchange their certificates (CPC and transaction record) to make sure that they conduct transaction with the known-entities. In this phase, type of entity is identified as the consideration to calculate trust. The rating of V_F is also calculated in order to determine local trust value of V_F as described in the following sub-section.
2) **Authentication and Pairing**. Based on CPC, they need to do authentication and pairing to create new session key by using the previous CSC parameters and J-PAKE method as elaborated in [19].
3) **Bidding process**. After recognizing each other, they then proceed with bidding-agreement as the compensation of transaction in case any of them violate the transaction by launching malicious activities.

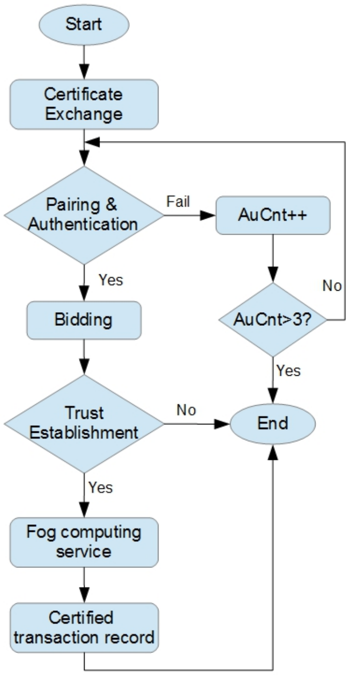

Fig. 2. Flowchart of the proposed method

4) **Trust establishment**. This phase attempts to decide whether to continue fog computing transaction or not by considering several parameters as described in the following sub-section. If mutual trust is achieved by both parties, then trust establishment for current fog computing service is considered to be successful.
5) **Fog computing service transaction**. In this phase, V_C will upload some data or offload some computations to V_F. To simplify the system model, we assume that V_F behaves honestly to keep data and computation request and not to disclose them to another vehicles.
6) **Certified-transaction-record**. The transaction is ended by issuing both-signed-transaction-record and putting it into their blockchain of evaluation record as done by [20]. By putting transaction record into blockchain as done by [20], both vehicles are assumed to be unable to forge or tamper the transaction record.

B. Trust Establishment

As the integrated system, trust establishment on vehicular fog system cannot be separated from the security system of infrastructure-based fog computing service. Even though trust is decided by only both V_C and V_F on the infrastructure-less area without intervention of FN, yet the role of FN is still needed to monitor behavior of both V_C and V_F interaction by mean of analyzing the certified-transaction record that is submitted to FN whenever both V_C and V_F are encountering network infrastructure.

Then, trust is calculated by considering local transaction on rural area and also global transaction with FN after entering infrastructure-supported area. Local trust is used to decide whether fog computing service transaction on rural area is feasible and secure. Meanwhile, global trust calculation is conducted to collect data from V_C, V_F, redeem compensation from malicious activities and to evaluate the performance of each entities. However, due to limited space of this paper, the global trust calculation, including how to authenticate V_C, V_F, certified-transaction record, and also how to hand over data from V_F to FN, will be discussed in the future for better understanding.

In the case of local transaction between V_C and V_F, trust is decided based on entity type, bidding number, and record of transaction. All parameters are combined by putting weight on each parameters to determine the priority of trust calculation as stated in the following equation.

$$LT_{ij} = \begin{cases} w_e + w_b\widehat{B_j} & \text{if } i = V_F \\ w_e + w_b\widehat{B_j} + w_r\widehat{R_j} & \text{if } i = V_C \end{cases} \quad (1)$$

Thus, LT_{ij} is the local trust calculated by vehicle-i for vehicle-j. Note that i, j can be any vehicles either V_F or V_C because local trust is calculated by both vehicles. The data weight on that equation is composed of weight of entity w_e, weight of bidding w_b, and also weight of record w_r as defined in the following equations.

$$w_e = \begin{cases} 0.6 & \text{if public-owned vehicle} \\ 0.4 & \text{if private-owned vehicle} \end{cases} \quad (2)$$

$$w_b = \begin{cases} 0.4 & \text{if } Max(B_i, B_j) < \Delta C_j \\ 0 & \text{if } Max(B_i, B_j) > \Delta C_j \end{cases} \quad (3)$$

$$w_r = \begin{cases} 0.2 & \text{if } |R| \geq 0 \\ 0 & \text{if } |R| = 0 \end{cases} \quad (4)$$

Note that, public-owned vehicle is given higher priority due to its purpose to serve citizen as compared to private-owned vehicle. As for weight of bidding, after each vehicles propose their bidding, the average bidding value is calculated as $\overline{B_{ij}}$. Then, that average value will be compared with the remaining digital currency (ΔC_j) of the pair-to-be vehicle. In this kind of situation, if vehicle V_j is potentially unable to pay compensation, then the transaction will not be proceeded. Lastly, weight of record is used to assess local trust of V_F regarding its service performance to V_C.

The parameters $\widehat{B_j}$ and $\widehat{R_j}$ are defined as the normalized bidding value from the pair and the normalized rating value from the pair respectively. Those value are derived from the following equations.

$$\widehat{B_j} = \frac{B_j}{Max(B_i, B_j)} \quad (5)$$

$$\widehat{R_j} = \frac{\overline{R_j}}{R_{Max}} \quad (6)$$

TABLE I
PARAMETERS OF SIMULATION

No	Parameters	Value
1	Length of road passing through rural area (km)	100
2	Number of village	9
3	Distance between village (km)	10
4	Max digital currency	1000
5	Bidding price	200 - 600
6	Payoff	0 - 500
7	Threshold of trust for V_C	0.6
8	Threshold of trust for V_F	0.7

After calculating trust, vehicle then decide to continue ad-hoc fog computing service if LT_{ij} value is equal or bigger than the defined threshold. In this paper, threshold of local trust is adjustable, yet the default value is defined as 0.6 for V_C and 0.7 for V_F which is derived from mean trust value. Eventually, vehicular fog computing service transaction is enabled if both V_C and V_F can be trusted by each other after trust calculation.

III. Experimental Result

In this section, we will present the benefit of applying our trust establishment method in rural area by mean of simulation through repeated data sampling by considering the interaction and behavior of both V_C and V_F in conducting vehicular fog computing service in infrastructure-less area. This game will also include the role of FN that is installed on some villages by assuming that authentication process is done among FN, V_C, and V_F, and also both V_C and V_F are honest entities that will not forge the information on certified-transaction record. Thus, FN will only need to decide the amount of payoff that will be given to V_C and V_F if any malicious activities, rule violation, and/or attacks are detected. The payoff in this scheme will be used to limit the number of transaction that can be potentially harmful for both V_C and V_F.

As for increasing clarity of experiment and understanding the given parameters in Table I, let us consider there is a rural area in somewhere around earth that the length of road spans about 100 km passing through that rural area. While traveling through that rural area, vehicle may meet or visit several villages which are separated by10 km in distance. At the village, network and computing infrastructures are installed including FN from several infrastructure-based fog computing service provider (or let's say from telecommunication service provider).

When meeting with a village, vehicles then submit certified-transaction record to FN. Then, as the response of that record, we consider to use payoff as the feedback of the following vehicular fog computing service. After checking the transaction record, FN will issue the new digital currency by considering the existence of rule violations or malicious activities that are conducted by both V_C and V_F. In case of conducting violations, the new issued digital currency will be reduced by the amount of payoff as given in that table. Lastly, this simulation is conducted by considering three types of vehicles, which are honest vehicles, opportunist vehicles (50% honest and 50% malicious), and also malicious vehicles.

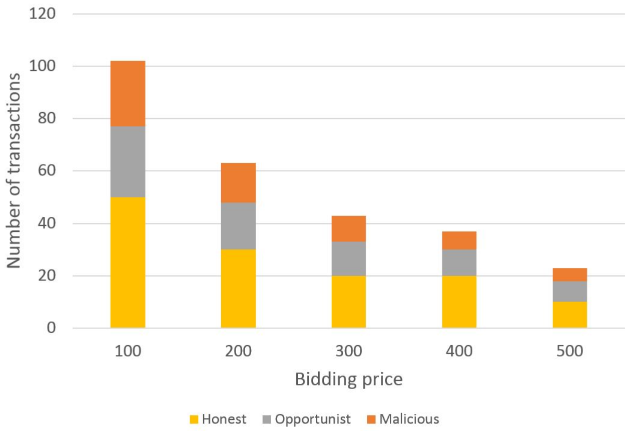

Fig. 3. Number of transaction with respect to bidding price

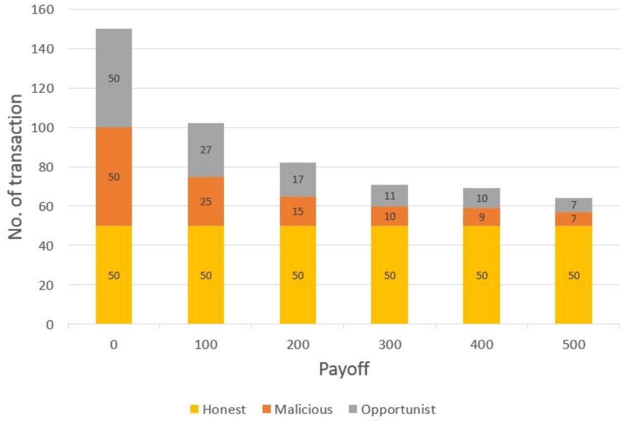

Fig. 4. Number of transaction with respect to payoff value

Then, simulation result is given in Figure 3 that describe the correlation between the usage of several value of bidding price toward number of transaction. In that figure, it is clearly depicted that number of transactions can be decreased if bidding price are increased. As for giving better understanding, let's say bidding price proposed by V_C is 200 and this price is also agreed by V_F, then in this situation both V_C and V_F may have up to five times transaction by considering the owned digital currency is 1000. In this case, as for greedy opportunist vehicles/attackers, their chance to commit much number of computing service transaction will be limited if their pair-to-be throwing higher amount bidding price.

Similar correlation between payoff value and number of transactions are shown in Figure 4. By using the same bidding price value, we can simply understand that payoff value will affect the number of transactions for malicious and opportunist vehicle due to evaluation process that is done by FN when vehicles passing through network-infrastructure-supported vil-

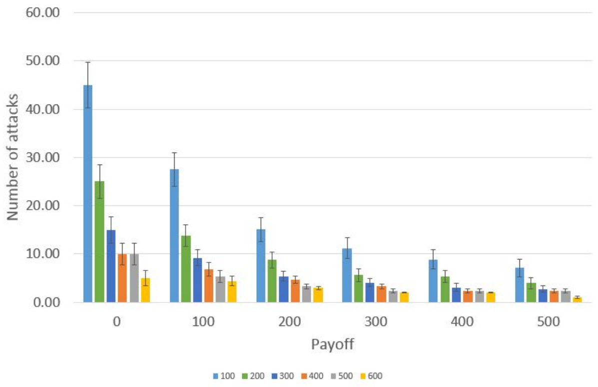

Fig. 5. Number of attacks with respect to bidding price and payoff value

lage. However, the same situation does not occur on honest vehicle which makes this method effective for back end of intrusion detection system based on behavior observation.

In case of combining bidding price and payoff as shown in Figure 5, we can see that the effect of bidding price is amplified by applying payoff for malicious vehicles. It is caused by the decreasing of next amount of digital currency of malicious vehicle with respect to the payoff price whenever meeting with the FN on network infrastructure-covered area of village. As a result, for vehicles that launch malicious activity, their chance to have transaction is decreased by limiting the digital currency. After several transaction and reporting to FN, we can eliminate the existence of vehicles that possibly launch malicious activities. As a result, we expect that vehicle may not hesitate to support other vehicle with lower computational resource because the system is able to suppress the potency of attacks and at the same time V_F will get compensation price for the loss or damage of its computational resource.

Lastly, this method combines the participation of both vehicles and FN in order to protect vehicular fog computing resource properties. Vehicles may increase the bidding price that enable fog computing service transaction to limit the transaction and also to gain compensation from attackers in case of experiencing attacks or malicious activities. To effectively increase the trust, FN also need to apply payoff to the attackers in order to decrease their chance to have transaction and launch malicious activities. By limiting and eliminating attackers participation in the vehicular fog computing service, we can create trusted environment and attracting more vehicles to participate and sharing their computational resources.

IV. Conclusions and Future Work

This paper presented a method to establish trust between client and service provider of vehicular fog computing service in the case of rural area environment which consists of network infrastructureless area and network infrastructure-covered area. The method only allows registered vehicles to conduct vehicular fog computing service transaction by issuing certificate to the vehicles prior to entering rural area. As a result, vehicles might only conduct vehicular fog computing service with authorized entities and also are protected from unknown/anonymous/outsider attacks. In order to provide mutual trust between vehicle client and vehicle-as-a-infrastructure of fog computing service provider, this paper proposed bidding price-based transaction (BPT) approach to limit the number of transaction with malicious entities and at the same time the BPT approach was used as the compensation for receiving malicious actions/violations. Then, simulation result showed that this proposed method is effective for decreasing the amount of attack by increasing the amount of bidding price and payoff.

For the future work, we attempt to extend this work by elaborating more on how to authenticate certified-transaction record on infrastructure-based fog node by considering both V_C and V_F are not honest in reporting their transactions. Some priority schemes on the BPT approach will also be discussed by considering history of malicious activities, proximity, and also sensitivity of the information. We also provide more detail architecture of the system that may enable the BPT approach to be applied in rural area.

Acknowledgments

The first author is partly supported by LPDP (Indonesia Endowment Fund for Education), Kementrian Ristek-Dikti (Ministry of Research, Technology, and Higher Education of Republic of Indoneia), Kanazawa University, and also Telkom University.

References

[1] O. Consortium, “Openfog reference architecture for fog computing,” OpenFog Consortium, Tech. Rep., 2017. [Online]. Available: https://www.openfogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL-1.pdf

[2] F. Yang, J. Li, T. Lei, and S. Wang, “Architecture and key technologies for internet of vehicles: a survey,” *Journal of Communications and Information Networks*, vol. 2, no. 2, pp. 1–17, Jun 2017. [Online]. Available: https://doi.org/10.1007/s41650-017-0018-6

[3] E. Ndashimye, S. K. Ray, N. I. Sarkar, and J. A. Gutirrez, “Vehicle-to-infrastructure communication over multi-tier heterogeneous networks: A survey,” *Computer Networks*, vol. 112, pp. 144 – 166, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128616303826

[4] M. Mouton, G. Castignani, R. Frank, and T. Engel, “Enabling vehicular mobility in city-wide ieee 802.11 networks through predictive handovers,” *Vehicular Communications*, vol. 2, no. 2, pp. 59 – 69, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209615000108

[5] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, “Vehicular fog computing: A viewpoint of vehicles as the infrastructures,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 6, pp. 3860–3873, June 2016.

[6] J. Kedieng Fendji and J. Nlong, “Rural wireless mesh network: A design methodology,” *International Journal of Communications, Network and System Sciences*, vol. 8, pp. 1–9, 2015.

[7] S. Chaklader, J. Alam, M. Islam, and A. S. Sabbir, “Bridging digital divide: ’village wireless lan’ , a low cost network infrastructure solution for digital communication, information dissemination & education in rural bangladesh,” in *2013 2nd International Conference on Advances in Electrical Engineering (ICAEE)*, Dec 2013, pp. 277–281.

[8] Y. Liu, C. Xu, Y. Zhan, Z. Liu, J. Guan, and H. Zhang, “Incentive mechanism for computation offloading using edge computing,” *Comput. Netw.*, vol. 129, no. P2, pp. 399–409, Dec. 2017. [Online]. Available: https://doi.org/10.1016/j.comnet.2017.03.015

[9] Y. Sun and N. Zhang, “A resource-sharing model based on a repeated game in fog computing,” *Saudi Journal of Biological Sciences*, vol. 24, no. 3, pp. 687 – 694, 2017, computational Intelligence Research & Approaches in Bioinformatics and Biocomputing. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1319562X17300529

[10] B. Xiao, B. Yu, and C. Gao, “Detection and localization of sybil nodes in vanets,” in *Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks*, ser. DIWANS ’06. New York, NY, USA: ACM, 2006, pp. 1–8. [Online]. Available: http://doi.acm.org/10.1145/1160972.1160974

[11] S. Park, B. Aslam, D. Turgut, and C. C. Zou, “Defense against sybil attack in vehicular ad hoc network based on roadside unit support,” in *MILCOM 2009 - 2009 IEEE Military Communications Conference*, Oct 2009, pp. 1–7.

[12] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, “Privacy-preserving detection of sybil attacks in vehicular ad hoc networks,” in *2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking Services (MobiQuitous)*, Aug 2007, pp. 1–8.

[13] Y. Hao, J. Tang, and Y. Cheng, “Cooperative sybil attack detection for position based applications in privacy preserved vanets,” in *2011 IEEE Global Telecommunications Conference - GLOBECOM 2011*, Dec 2011, pp. 1–5.

[14] X. Feng, C.-y. Li, D.-x. Chen, and J. Tang, “A method for defensing against multi-source sybil attacks in vanet,” *Peer-to-Peer Networking and Applications*, vol. 10, no. 2, pp. 305–314, Mar 2017. [Online]. Available: https://doi.org/10.1007/s12083-016-0431-x

[15] N.-W. Lo and H.-C. Tsai, “A reputation system for traffic safety event on vehicular ad hoc networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, p. 125348, Dec 2009. [Online]. Available: https://doi.org/10.1155/2009/125348

[16] T. R. Oliveira, C. M. Silva, D. F. Macedo, and J. M. S. Nogueira, “Snvc: Social networks for vehicular certification,” *Computer Networks*, vol. 111, pp. 129 – 140, 2016, cyber-physical systems for Mobile Opportunistic Networking in Proximity (MNP). [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128616302778

[17] R.-I. Ciobanu, R.-C. Marin, C. Dobre, and V. Cristea, “Trust and reputation management for opportunistic dissemination,” *Pervasive and Mobile Computing*, vol. 36, pp. 44 – 56, 2017, special Issue on Pervasive Social Computing. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1574119216302395

[18] S. Li, M. A. Maddah-Ali, and A. S. Avestimehr, “Coding for distributed fog computing,” *IEEE Communications Magazine*, vol. 55, no. 4, pp. 34–40, April 2017.

[19] M. Abdalla, F. Benhamouda, and P. MacKenzie, “Security of the j-pake password-authenticated key exchange protocol,” in *2015 IEEE Symposium on Security and Privacy*, May 2015, pp. 571–587.

[20] P. Otte, M. de Vos, and J. Pouwelse, “Trustchain: A sybil-resistant scalable blockchain,” *Future Generation Computer Systems*, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17318988