BPT Scheme: Establishing Trusted Vehicular Fog Computing Service for Rural Area Based on Blockchain Approach

Favian Dewanta, *Member, IEEE*, and Masahiro Mambo, *Member, IEEE*

***Abstract*—Passing through a rural area with a limited network infrastructure may disrupt fog computing support for vehicles. As a result, some applications on vehicles may turn off and bother the performance of the vehicular systems. In order to escape from this kind of situation, vehicular fog computing is discussed in recent times as an alternative of fog computing support while passing through a blank spot of network infrastructure. However, it is not feasible to establish a trusted vehicular fog computing service among vehicles without mutual trust. To deal with this situation, this paper proposes a method called Bidding-Price-based Transaction (BPT) for vehicular fog computing service in rural areas. This method is composed of bidding-price-based mutual trust establishment between client vehicle and server vehicle and also payoff assignment based on transaction evaluation. By applying this method, trusted fog computing service transactions between two vehicles can be achieved without the direct assistance of any trusted third party as a validating entity. The simulation results and feasibility analysis then validate the performance of the BPT scheme in rural areas. Based on feasibility analysis, we claim that the BPT scheme can be realized by adjusting vehicle speed and transmission range with respect to the size of offloaded data.**

***Index Terms*—Fog computing, rural area, trust establishment, vehicular network.**

I. Introduction

FOG computing service in the vehicular network has emerged as a main concept to support the implementation of the intelligent transportation system. Due to the latency issue, processing a huge amount of data generated by vehicles on a cloud server is not an appropriate solution for the vehicular network [1], [2]. Several ideas are introduced to solve the latency issue, including installing fog/edge computing servers close to the vehicle as a proxy of the cloud server [3], [4].

Utilizing standby computational resources of vehicles as the fog computing infrastructure in [5] is a fresh concept on realizing fog computing for vehicular network-based applications. Through this work, the paradigm of a vehicular fog computing system is not only applied on eNode-B or roadside unit (RSU) [6]–[8], but it can also be applied on vehicle-based computational resources [9], or even computational resources from others [10], such as privately owned cafes, houses, offices, shopping mall, etc. As a result, vehicular fog computing service is not only limited to the urban area but also available for the rural area by means of other vehicles' computational resources or reputable privately owned facilities' computational resources.

A rural area offers a unique environment, such as sparse population distribution, less energy sustainability, and low data traffic. As a result, deploying network infrastructure in rural areas is considered a high cost in terms of initial investment and continuous maintenance. To deal with those kinds of situations, some works in certain countries propose providing low-cost network infrastructure through the wireless mesh network [11] or village wireless LAN [12]. In other words, it can be implicitly inferred that vehicle-based fog computing service is more appropriate to be applied in rural areas as introduced in [5].

Several works discuss how to attract vehicle with rich computational resources to participate in general fog computing services. Liu *et al.* [10] present a method to extend cloud computing service by utilizing edge computing resources in several crowded areas, such as the railway stations, shopping malls, and airports. They encourage edge computing owners to participate in giving computation offloading service to mobile users. Meanwhile, Yan *et al.* [13] discuss an algorithm to integrate sporadic computational resources in the local network utilizing a dynamic resource pool in order to perform assigned tasks by the fog broker. Their simulation results proved that their crowd-funding algorithm could decrease the service level agreement (SLA) violation rate and also accomplish assigned tasks faster in comparison with the other two algorithms (MM and MBFD).

In order to attract the participation of prospective vehicles with rich computational resources and also to give security and privacy assurance to the client vehicles, this paper proposes Bidding-Price-based Transaction (BPT) for vehicular fog computing service in rural areas. This method is constructed by using bidding-price, which can be seen as the service cost and also compensation cost at the latter part of global trust evaluation, and also blockchain approach as local trust enabler of fog computing service transaction. To eliminate adversaries in the system, this method also utilizes the concept of payoff from

Manuscript received October 14, 2019; revised June 5, 2020, October 13, 2020, and December 28, 2020; accepted January 3, 2021. Date of publication January 13, 2021; date of current version March 10, 2021. The review of this article was coordinated by Prof. S. De. *(Corresponding author: Favian Dewanta.)*

Favian Dewanta is with the School of Electrical Engineering, Telkom University, Bandung 40257, Indonesia, and also with the Division of Electrical Engineering and Computer Science, Graduate School of Natural Science and Technology, Kanazawa University, Ishikawa 920-1192, Japan (e-mail: favian@telkomuniversity.ac.id).

Masahiro Mambo is with the Faculty of Electrical, Information and Communication Engineering, Institute of Science and Engineering, Kanazawa University, Ishikawa 920-1192, Japan (e-mail: mambo@ec.t.kanazawa-u.ac.jp).

Digital Object Identifier 10.1109/TVT.2021.3051258

the game theory, which is performed by infrastructure-based fog nodes. Eventually, by combining the bidding-price, blockchain approach, and payoff method, vehicles are likely to be feasible to have fog computing service transactions while traveling through rural areas without the presence of fixed network infrastructures (eNodeB/RSU) and trusted third parties.

In this paper, our contribution can be summarized as follows.

- First, we describe the most relevant related work considering authentication issues, evaluation of reputation, and blockchain approach in vehicular networks. At the end of related work studies, we formulate our motivation and general concepts of the BPT scheme, and also deliver features comparison in trust establishment for rural areas.
- Second, we incorporate trusted vehicular fog computing service considering the situation of network infrastructure absence in a rural area in order to attract the participation of vehicles with rich computational resources. For that purpose, we apply the BPT scheme to establish mutual trust between client vehicle and server vehicle based on local trust and global trust evaluations.
- Third, we provide security analysis against several known malicious attacks concerning the most relevant previous works in order to demonstrate the strength and efficiency of our scheme.
- At last, we conduct feasibility analysis against vehicle movement parameters, e.g., speed, density, and transmission range, in order to demonstrate that our BPT scheme is theoretically solid prior to conducting practical experiments using a real testbed. Moreover, several related works are analyzed in the simulation part for enhancing the discussion part, especially the advantages and disadvantages of our BPT scheme.

II. Related Work

Trust establishment is a broad area that covers various factors, including security, safety, reliability, resilience, and privacy, as elaborated in [14]. Some other works discuss the trust as a result of evaluating reputation/recommendation, verifying and authenticating entities/data, and performing good behavior by using weight-based evaluation as discussed in [15]–[17]. Meanwhile, Guo *et al.* [18] classify and elaborate several types of trust computations in any environment by considering composition, propagation and aggregation method, update scheme, and formation of the trust among entities involved in the environments. The following subsections present the related work and the motivation of our work.

A. Authentication of Entities

Several works propose public key infrastructure (PKI) techniques to verify Sybil vehicles and eventually obtain trusted information from a correct entity. As an example, Xia *et al.* [19] enhance the previous work on event-based reputation systems [20] by adding a centralized authentication system based on PKI to verify sources of information. In another similar work, Lee *et al.* [21] utilize a session key-based certificate (SKC) approach to detect Sybil attacks and protect private information simultaneously. This method relies on the presence of Trusted Third Parties (TTP) to generate session keys and verify malicious vehicles. However, we can argue that centralized techniques based on TTP may suffer from a higher amount of overhead data, a slow response time of services, and also compromised TTP. Moreover, in the time of TTP absence as occurring in rural areas, centralized techniques are not relevant and reliable anymore to protect vehicles from attackers and malicious activities.

In [22], Mutaz *et al.* investigate the traffic of vehicles which always submit reports to RSU. This scheme is unique because of its approach in exploiting model of physical parameters on transportation engineering, e.g., platoon dispersion, speed of vehicles, etc., and also combining with Sybil attack detection schemes, which are similar with [23] and [24] in some way to verify physical presence of the vehicles. However, verifying the physical presence of vehicles relies on the presence of infrastructure, which is infeasible for a rural area.

Another method for authenticating entities employs a decentralized technique as proposed by Dua *et al.* [25]. Their method utilizes a two-level authentication key exchange scheme using elliptic curve cryptography. At the first level, authentication occurs between a certificate authority (CA) and a vehicle taking the role of a cluster head (CH). The second level is between CH and the rest of the vehicles on the road. To validate the security aspect of their proposed scheme, several formal methods are conducted, including the use of BAN Logic, random oracle model, and AVISPA software. The results are excellent in terms of protection against several known attacks under Dolev-Yao and CK adversary models [25]. However, to the best of our knowledge, vehicular fog computing service not only requires secure message communication protocol but also needs to create a vehicular evaluation system in the way of giving rating value, e.g., good, moderate, bad, etc., and providing incentive in order to attract vehicles participation and eliminating insider attacks.

In the following year, Yao *et al.* [26] discuss establishing reliable and secure vehicular fog service (VFS) provision to client vehicles. Their proposal extends the idea of vehicular fog computing, as initially elaborated by Hou *et al.* [5], by incorporating a mechanism that consists of vehicular fog (VF) construction method and VFS access method. In the latter part, based on analysis simulation results, they claim that their method can ensure connectivity while conducting container live migration, guaranteeing message integrity, and also providing security for vehicles and containers. However, since their proposal requires RSU's role to authenticate client vehicles in the VFS access method, their mechanism of reliable and secure VFS is not likely to fit the application in rural areas due to the less-network infrastructure issue. Moreover, in the absence of service feedback and reward-punishment scheme, it is difficult for client vehicles to trust server vehicles regarding the quality of service. At the same time, it can decrease the participation of server vehicles to share their computational resources.

B. Evaluation of Reputation

This trust establishment offers different points of view in which trust should be established by using evaluations of

reputations on the basis of the social network interaction model. Under the model, each entity should communicate with as many entities as possible to obtain more accurate verification and reputation calculation. By considering majority opinions from others, Ciobanu *et al.* [27] investigate the security aspects of employing intermediate nodes on the delay-tolerant network (DTN). They propose opportunistic trust and reputation management called SAROS in order to detect and avoid malicious nodes by comparing several contents coming from various nodes within an interest-space. Once a different message content is detected by a receiver node, the nodes involved in that particular transmission chain, i.e., from a publisher node to the receiver, will be assigned a bad reputation. In [28], a different approach using a social network approach is proposed by Thiago *et al.* This work relies on certification graph establishment and reputation evaluation among vehicles as the authentication process of message exchange and transmission. Their simulation results show that increasing the number of friends can increase the number of reliable messages in an opportunistic vehicular network. However, intuitively trust computation that relies on the number of participants is vulnerable to collusion attacks. Moreover, without verifying entities, e.g., identity, location, etc., the previous trust evaluations in [27] and [28] will be useless in case of adversaries launching Sybil attacks.

Concerning PKI-based application in a multi-agent-system, a peer evaluation approach called certified reputation (CR) is proposed by Huynh *et al.* [29]. This work also considers not only direct evaluation of other entities but also third-party references in order to present more accurate evaluations against bad-mouthing attacks, ballot-stuffing attacks, and collusion attacks. In several years later, that work is improved by Liu et al. [30] by adding cross-domain features called lightweight cross-domain trust (LCT) model for solving improper similarity weight calculation in case of no previous interaction between trustor and trustee. However, we can argue that those CR and LCT methods can suffer from impersonation attacks due to the absence of entities' verification. Moreover, considering the demographic aspect and the sparse number of vehicles passing a rural area, their work becomes more vulnerable due to difficulty to verify trust certifications without the existence of other vehicles in a group or roadside unit as a PKI.

C. Blockchain-Based Transaction Record

Blockchain technology emerges as a method that offers decentralization of authentication, transparency in any transaction, and also security from any known attacks. Its application varies from cryptocurrency, industrial automation and control systems, and medical record [31]. It promotes multiple nodes as an equal verifier instead of a single-node verifier, which can avoid compromised TTP attacks. A usage of consensus algorithm in blockchain among verifiers may mitigate risks of transaction record manipulation launched by malicious nodes. Moreover, nowadays, blockchain is offered as a package of service called NutBaaS, which monitors and maintains service in cloud computing, as discussed in [32]. As a consequence, it can be easily deployed in any cloud computing-based system, and a user needs only focus on the business aspect without spending much time on the technical aspect.

Despite its excellent property in delivering secure transactions, blockchain is not always assumed to be fully secure due to the existence of a majority of malicious groups that may tamper with transaction records [33]. That malicious ledgers group can potentially destroy immutability property in blockchain in which it may create devastating damage and degrade trust among users. However, we do not focus on blockchain attacks because ledgers/verifiers in this research are assumed to be trusted and honest in delivering transaction verification.

As a powerful authentication method, blockchain is also used in edge computing-based Internet of Things as discussed in [34]. It creates a secure connection and authentication by means of a smart contract combined with asymmetric cryptography. As for realizing the blockchain system, the authors create separate layers and put blockchain in the third layer for storing terminal information and generating smart contracts over Hyperledger Fabric. However, this blockchain approach requiring an online network to verify every transaction does not fit with the condition of the rural area, which possesses poor network infrastructure.

Regarding the vehicular network, Yang *et al.* [35] discuss the application of blockchain for traffic event validation and trust verification. The work collects traffic events, e.g., locations, speeds, etc., in order to detect overspeeding or emergency braking. In order to enable anonymous identity, the authors apply public key infrastructure in their work for verifying entities, providing tamper-proof keys, and non-repudiation properties. Proof of event procedures is carried out for validating events before storing events in the global blockchain. Regardless of their excellent results in detecting fraudulent events, to the best of our knowledge, the approach is not appropriate for the rural area due to requiring massive network infrastructures. Moreover, their work does not provide a secure channel, which is important for protecting data transfer in vehicular fog computing services.

In order to take advantage of blockchain property in a rural area, we adopt the concept of carry protocol [36], which is applied in South Korea by a company named Carry that connects offline merchants and customers using blockchain. The carry protocol sets two types of blockchains, which are offline and online blockchain. The offline blockchain, managed by carry device API and carry wallet API, is carried out by users for offline transactions with the offline merchant by entering a phone number or scanning QR code. The users can manage their cryptocurrency offline and possibly make it online with some degree of privacy protection by uploading their blockchain for receiving CRE reward (cryptocurrency from carry protocol). However, their method is not considered as a fully offline approach since their transactions require validation from the carry blockchain server through the internet network.

D. The Motivation of Our BPT Scheme

The work discussed in this paper is a part of our project for establishing trusted communication in fog computing-based vehicular networks in the urban scenario [37] and rural scenario [38]. In the previous work [38], we show that our BPT scheme is effective in mitigating the risk of attacks in a rural

TABLE I
INTUITIVE COMPARISON OF FEATURES IN TRUST ESTABLISHMENT PROPOSAL

Trust Models	F1	F2	F3	F4	F5
SNVC [28]	✓	✓	×	×	×
SAROS [27]	✓	✓	×	×	×
Dua et al. [25]	✓	×	✓	✓	×
Yao et al. [26]	✓	×	✓	✓	×
Yang et al. [35]	×	×	✓	×	✓
Our	✓	✓	✓	✓	✓

F1: Decentralized/Distributed approach; F2: Reputation-based evaluation;
F3: Authentication of identity/behavior/etc.;
F4: Secure channel establishment;
F5: Blockchain-based transaction record;
✓: Available; ×: Unavailable.

area by means of a Game Theory simulation scheme. However, it means nothing if the BPT scheme cannot be realized in a real situation considering the computational and communication cost of the BPT scheme with respect to properties of the vehicular network in a rural area. Thus, this discussion extends our previous work [38] with the purpose of investigating the feasibility of applying the Bidding-Price-based Transaction (BPT) scheme in a rural area. The feasibility of our work in Section V is elaborated on the basis of physical characteristics, e.g., vehicle speed, vehicle density, and transmission range, and also computational and communication cost with respect to tight connection time maintained by dynamic vehicles movement on the road. In addition to the feasibility analysis, our work at present is also different with respect to [38] in such a way that several possible attacks, which are not clearly mentioned in previous work, are explicitly raised and analyzed in Section IV. Therefore, the issues and discussions are more vivid and closer to the real situation of the vehicular network in a rural area.

We consider several works at the previous subsections which fit the condition of a rural area. Those mentioned work, as listed in Table I, share the same mobile ad hoc / peer-to-peer communication approach and also a similar distributed trust establishment approach. Even though the related work can be applied in a rural area, they still possess some vulnerabilities that the attackers can exploit. As for authentication approaches, they enable secure communication among all legitimate vehicles, but they cannot attract vehicles with a high level of computational resources to participate in vehicular fog computing service as presented by Dua *et al.* [25] and Yao *et al.* [26]. As for the evaluation of reputation approaches, SNVC [28] and SAROS [27] can relatively deliver objective evaluation among vehicles in an opportunistic (disruption-tolerant) network and concurrently identify malicious vehicles. However, they require high exposure to the social network connections in such a long time to perform an optimal evaluation in which the high exposure of social network connection is not feasible in the rural area. Finally, the blockchain-based trust establishment approach seems perfect for rural areas due to its tamper-proof transaction record and distributed trust establishment properties, as demonstrated by Yang *et al.* [35]. However, they require a fixed identity and certificate all the time in order to conduct transactions, in which it is susceptible to the attack of tracing vehicle trajectory through their identity/certificate.

TABLE II
SYMBOLS USED IN THE BPT SCHEME DISCUSSION

Symbol	Description
TA	Trusted authority
V_C, V_F	Client vehicle and fog computing server vehicle
FN	Fog node located in base station / road side unit
CPC	Certified public credentials
ID	Identity of a vehicle assigned by the TA
PK	Public key of a vehicle assigned by the TA
C	Currency of a vehicle assigned by the TA
$Sign_p$	Signature of the CPC assigned by the TA
CSC	Certified secret credentials
SK	Secret key of a vehicle assigned by the TA
j	Juggling key of a vehicle assigned by the TA
G	Sub-group of a vehicle assigned by the TA
g	Generator of the sub-group G assigned by the TA
$Sign_s$	Signature of the CSC assigned by the TA
CTR	Certified Transactions Record
r_{cf}	Transaction rating given by V_C to V_F
p_c	Hash of previous transaction record in V_C
hd_c	Hash of offloaded data / computational trace of V_C
C_c^{rem}	Remaining currency owned by V_C
t_c	Timestamp recorded by V_C
σ_c	Signature of transaction receipt created by V_C
C_f^{rem}	Remaining currency owned by V_F
t_f	Timestamp recorded by V_F
B_{cf}^{fn}	Final bidding price selected by V_C and V_F
p_f	Hash of previous transaction record in V_F
σ_f	Signature of transaction receipt created by V_F

In this paper, we present a concept of establishing trusted vehicular fog computing service by incorporating three prominent aspects, which are 1) entities authentication and session key generation employing J-PAKE scheme [39], 2) the bidding-price-based transaction for mitigating the risk of attacks and attracting the participation of other vehicles, and 3) certified evaluation system by means of blockchain approach. The first and second aspects are done in the rural area as a local trust establishment between a client and a server vehicle. The last aspect is executed as a part of a global trust establishment. By applying the three aspects, a vehicle can perform vehicular fog computing service with another legitimate vehicle, and at the same time, it can attract another legitimate vehicle to share their computational resources. In addition, it is also able to objectively evaluate other vehicles by looking into certified transaction record-based on the blockchain, which is shared in the local trust establishment approach without any high exposure to the social network connection. In the last step, a vehicle can obtain a new identity and certificate by submitting their certified transaction record into a global blockchain managed by a number of fog nodes consortium. As a consequence, a vehicle can possess a property of inability to trace. Eventually, we summarize the features of our work in comparison with other most related work in Table I.

III. TRUST ESTABLISHMENT IN RURAL AREA

This section will discuss establishing a trusted vehicular fog computing service in the rural area. Prior to discussing the proposed method in detail, we provide Table II for describing

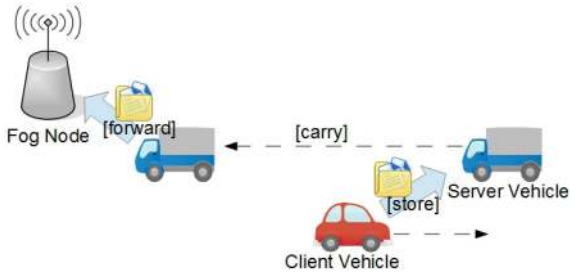

Fig. 1. Store-carry-and-forward scheme for fog computing service in a rural area.

notations or symbols used in explaining the concept of the BPT scheme.

A. Overview of Establishing Trusted Vehicular Fog Computing Service in Rural Areas

A rural area is often defined as a remote area with fewer inhabitants and far enough from urban areas. It can be desert area, forest area, mountain area, island area, and other similar areas with fewer network infrastructures in the point of view of network facilities. As for network providers, profit should be considered in order to expand their network coverage, whether profit generated in an area can cover installation and maintenance costs or not. As a consequence, there are some rural areas that can be only partially covered by network providers or even uncovered by any network provider.

Considering network coverage in a rural area, fog computing service based on fixed infrastructure, e.g., 4G-LTE, 5 G, WiMax, etc., is not appropriate for the vehicular network application. It can cause disruption of service in the middle of usage while moving away from the base station due to entering out of network coverage area. Even though fog computing service is not always necessary while driving, but it could lead to some serious issues if it is unavailable in some important cases.

For example, data storage for storing sensors, actuators, and application log run out while passing a rural area. Without offloading data to fog computing service, some important old data in the vehicle have to be overwritten with the newly captured data. In some cases, this situation can cause computational issues, e.g., a decrease in accuracy, precision, reliability, or even affect the driving experience if the vehicle's application relies on old data as a part of inputs.

To the best of our knowledge, this situation can be prevented if fog computing service (FCS) is not set to be fixed only in base station. As discussed by several researchers in [5] and [26], fog computing services can also be provided by other vehicles possessing higher computational resources. Thus, we attempt to employ other vehicles' computational resources as fog computing service providers that can temporarily store-carry-and-forward the data to the infrastructure-based fog computing service providers eventually, as given in Fig. 1.

However, it is not easy to simply select any random vehicle in a rural area to be a server vehicle that can perform store-carry-and-forward, especially for important, confidential,

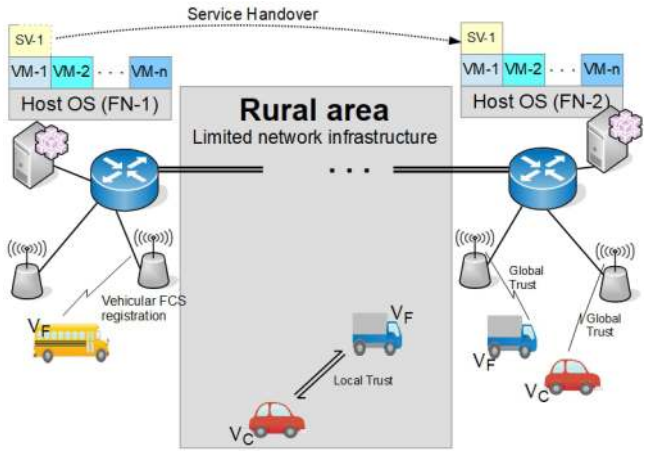

Fig. 2. Proposed local trust and global trust establishment in case of trusted third-party's absence.

sensitive, and private data. Unlike an urban area, a rural area does not have trusted authority that can authorize other vehicles as server vehicles. As a result, careless server vehicle selection can lead to severe issues related to data theft, privacy violation, or cyber-attack that can endanger the driver or passengers' security and safety. Thus, in order to enable vehicular fog computing service in unavailable network service rural area, there are four aspects that should be considered, which are (1) incentive as the way to attract the participation of rich computational resources' vehicles, (2) authentication as the procedure to identify trusted-authority (TA) authorized entities, (3) weight-based trust computation as the key to enabling transaction, and (4) certified transaction record as the accounting mechanism in order to update currency and detect violations from any vehicle.

In order to accommodate the four mentioned aspects, we propose the bidding-price-based transaction (BPT) scheme as a method to establish trust among vehicles and enable fog computing service in the absence of TA as occurring in the rural area. BPT scheme consists of two approaches: (1) local trust that enables fog computing service between server vehicle and client vehicle, and (2) global trust that evaluates certified transaction record and issues/revokes a pair of certificates for each vehicle. Note that local and global trust are not standalone activities; those trust computation should be accomplished to guarantee security and provide service at the same time.

Fig. 2 captures an overview of the BPT scheme activities. Prior to entering a rural area, vehicles are required to send a registration form to any fog node in order to obtain approval for conducting vehicular fog computing service. The result of the registration process is (1) certified public credentials (CPC) that are exchanged among vehicles prior to having vehicular FCS transactions and (2) certified secret credentials (CSC) that are used to authenticate TA-authorized vehicles and create certified transaction record (CTR). While passing the rural area, vehicles perform local trust establishment, including authentication, session key generation, and CTR creation. At the end of the BPT scheme session, both CTR and offloaded data are stored into the

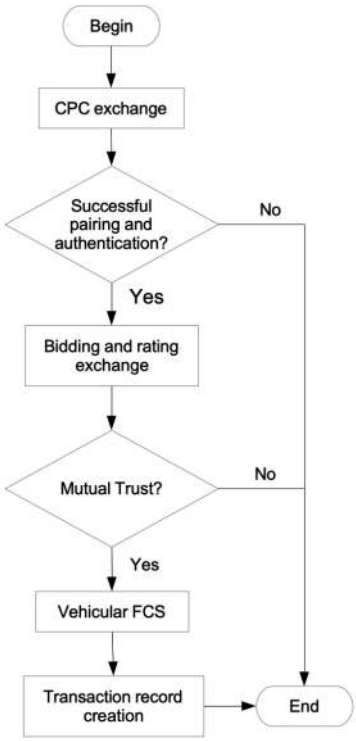

Fig. 3. Flowchart of Local Trust Establishment.

fog node, and then the fog node processes CTR in order to give incentive or punishment for each transaction.

Prior to elaborating on details, it is essential to reveal the registration process between a vehicle and TA. As a part of the fog computing service provided by the network provider, TA is located in the fog node and accessed if a vehicle registers to vehicular fog computing service either as a client or a server vehicle. After being authenticated by TA, the vehicle submits a digital currency C, including credit card or prepaid IC card, as a part of the registration process that is going to be used in vehicular FCS. Then, TA proceeds the request by issuing CPC $\langle ID, PK, C, Sign_p \rangle$ which mean identity, public key, currency, and signature of CPC signed by TA respectively. TA also issues CSC $\langle SK, j, G, g, Sign_s \rangle$, which mean private key, juggling key, sub-group G, generator g derived from Z_p^* with prime order q, and CSC signature from TA. Note that j, G, and g are adopted from J-PAKE [39] because it is proven as an effective and secure method for authentication and session key creation. Lastly, it is essential to mention that in the rest of the discussion, the term fog node and TA will be interchangeably used to refer to the trusted authority, which is part of fog node infrastructure.

B. Local Trust

After receiving CPC and CSC from TA, this mechanism establishes trusted vehicular FCS between server and client vehicles in a rural area, as shown in Fig. 3. Then, the detailed procedure is elaborated below.

- *CPC exchange* is executed at the beginning of local trust in order to obtain parameters for authenticating and pairing between two interacting vehicles.
- *Authentication and pairing* are intended to verify whether two communicating vehicles are authorized by TA to conduct vehicular FCS. In some cases, if this step is failed, it can be indicated that one of those two vehicles is an adversary. The end of this step is to create a session key that is used to protect communication between server and client vehicles.
- *Bidding and rating exchange processes* require two vehicles to propose the price for vehicular FCS and the compensation value after receiving any violation or attack. Alongside the bidding price exchange, those vehicles also declare their rating based on the blockchain-based transaction record. The final bidding price is determined by the maximum function.
- *Trust computation* considers parameters, which are entity type, proposed bidding price, and reputation prior to putting trust on other vehicles. Given Equation (1) shows trust computation, which is done by vehicle-i to vehicle-j for both server vehicle V_F and client vehicle V_C. In that equation, all vehicles need to consider the weight of entity w_e, the weight of bidding price w_b, and normalized bidding price $\widehat{B_j}$ as presented in Equation (2), (3), and (4). As for the client vehicle, it also has to consider the reputation of the server vehicle using the weight of rating w_r, average rating $\overline{R_j}$, and normalized rating $\widehat{R_j}$ as shown in Equation (5) and (6).

$$T_{ij} = \begin{cases} w_e + w_b \widehat{B_j} & \text{if } i = V_F \\ w_e + w_b \widehat{B_j} + w_r \widehat{R_j} & \text{if } i = V_C \end{cases} \tag{1}$$

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

$$\widehat{B}_j = \frac{B_j}{\mathrm{Max(B_i, B_j)}} \tag{3}$$

$$w_b = \begin{cases} 0.4 & \text{if } \mathrm{Max(B_i, B_j)} < \mathrm{C_j^{rem}} \\ 0 & \text{if } \mathrm{Max(B_i, B_j)} > \mathrm{C_j^{rem}} \end{cases} \tag{4}$$

$$w_r = \begin{cases} 0.2 & \text{if } |R| \geq 0 \\ 0 & \text{if } |R| = 0 \end{cases} \tag{5}$$

$$\widehat{R}_j = \frac{\overline{R_j}}{R_{\mathrm{Max}}} \tag{6}$$

To determine the state of trust, threshold value is set as 0.6 for V_C and 0.7 for V_F. Those threshold values are calculated from the mean trust value of V_C and V_F if w_e is equal to 0.4. As for V_C calculating trust value toward V_F, the mean trust value will be $T_{ij} = 0.4 + w_b \widehat{B_j} + w_r \widehat{R_j}$ in which the mean value of $w_b \widehat{B_j} = 0.2$ and $w_r \widehat{R_j} = 0.1$. In other words, for being trusted by the V_C, the V_F should provide information, i.e., vehicle type (w_e), bidding price (B_j), and rating of the previous transaction (R_j), to the V_C so that the trust value calculated by the V_C should be bigger than 0.7, the default threshold value for the V_F. As for V_F calculating trust value toward V_C, we can

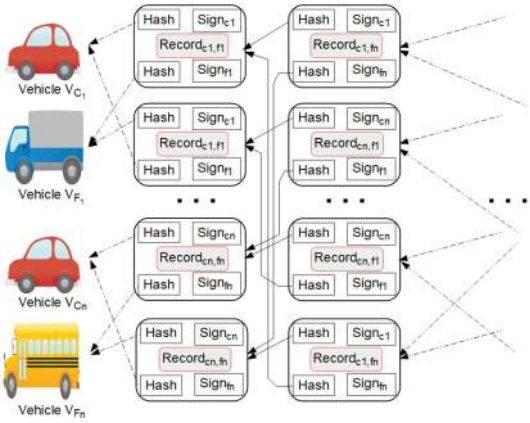

Fig. 4. Blockchain of certified transaction record.

derive the mean trust value of 0.6 points as similar to the previous explanation. However, those values of V_C and V_F are not fixed; rather, it can be customized for the sake of defining different levels of trust because each rural area possesses different levels of security threat. To the best of our knowledge, it is more appropriate to let users set different levels of V_F and V_C threshold according to their knowledge about local security issues. Eventually, having mutual trust between two vehicles is a must before continuing into vehicular FCS transactions.

- *Vehicular FCS transaction* is executed after both vehicles put trust in each other by conducting previous steps. This step should create a digest of computation at the end of this step to claim back the offloaded data in the vehicular FCS transaction.
- *Certified transaction record creation* is done after finishing vehicular FCS transactions. The creation of a certified transaction record (CTR) employs blockchain to bind all transactions as adopted from the TrustChain approach [40]. Fig. 4 visualizes the blockchain of CTR generated in this step. In this figure, each CTR block points to each previous CTR block and counter party's CTR block to create resiliency against denial of CTR and any other attack, which is explained in the security analysis part. In addition, due to applying the offline blockchain approach, each vehicle possesses the same CTR associated with vehicular FCS transactions.

C. Global Trust

This part reviews a part of the global trust procedure, primarily how to authenticate CTR submission from all vehicles while encountering fog nodes in a rural or urban area. Before discussing further, we need to clarify that this verification procedure is conducted using an ephemeral session key between vehicle and fog node to provide forward secrecy property and avoid path tracing from the adversary. Unlike local trust that is used to enable vehicular FCS and attract other vehicles to participate, this global trust purpose is (1) to verify CTR generated from vehicular FCS, (2) to assign reward and punishment/payoff for each vehicle, (3) to issue and revoke CPC and CSC. As for the punishment scheme, our previous work [38] discusses the effectiveness of applying bidding price and payoff values in eliminating malicious vehicles by means of the game theory approach.

In the BPT scheme, the global trust and local trust are like two sides of a coin. They possibly exist at the same time or one after another either in a rural/urban area. We can simply illustrate that the global trust is the baseline of our BPT scheme, which relies on local blockchain (in some other, work it is also called offline blockchain) and global blockchain. By saying local blockchain, it means the CTR that is kept by those server and client vehicles. It remains valid all the time until it is submitted to the fog node due to the new assignment of CSC and CPC. One may wonder whether local blockchain is feasible and trusted due to the absence of ledgers. We can argue that the local blockchain scheme is considered as a secure and trusted method as long as each block contains a pointer to the previous blockchain of a counter-party as discussed in work called Trustchain [40]. Even though the discussion in [40] does not explicitly assign Trustchain for a rural area, we can argue that employing Trustchain for achieving consensus only within two participants, instead of multiple ledgers, meets the requirement of trust establishment between server and client vehicles in a rural area.

As for global blockchain, it is the compilation of all CTR's which are submitted by all vehicles involved in the BPT scheme to the fog nodes. It remains valid all the time because, in this stage, the vehicles are recognized as a single identity even though their identities are dynamic in the local trust. Moreover, the global blockchain records behaviors of the vehicles, which can be used for further analyses related to payoff assignment, security, or safety aspects. However, this paper does not discuss the global trust in detail, such as how to handle offline blockchain in a rural area and how the ledger can verify and trace multiple transaction records generated by vehicular FCSs. Instead of that, we will provide separate discussions of those topics in future work. To give a few insights and soundness to this work, we provide a short discussion of global trust in the way of transaction record flow among a client vehicle, a server vehicle, and an RSU as given below.

1) Transaction Record Exchange: After conducting vehicular fog computing service transaction, V_C will issue a receipt of the transaction, which consists of the transaction rating r_{cf}, the hash of previous transaction record p_c, the hash of offloaded data / computational trace hd_c, the remaining currency C_c^{rem}, the timestamp t_c, the signature of receipt σ_c which is signed by using SK in CSC above. In the case of the first transaction, the hash of the previous transaction is calculated from CPC as the root of the previous transaction pointer.

Upon receiving transaction receipt $\langle p_c, r_{cf}, hd_c, C_c^{rem}, t_c, \sigma_c \rangle$, V_F checks the signature of that receipt by using the public key of V_C. If it is correct, then V_F recreates that receipt by adding the remaining currency C_f^{rem}, the timestamp t_f, final bidding B_{cf}^{fn}, the hash of the previous transaction record p_f, and also the signature of transaction record σ_f. In the case of the detection of the wrong signature, V_F requests another receipt.

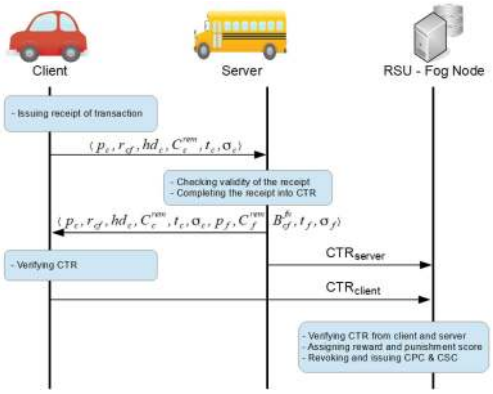

Fig. 5. CTR creation and submission flow.

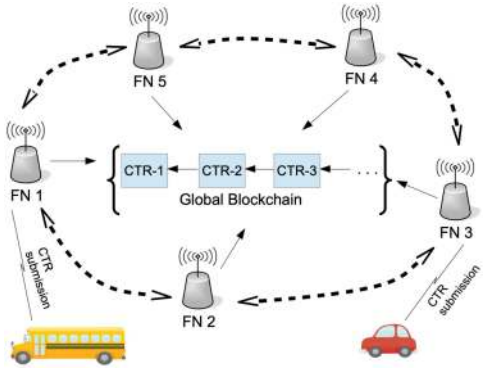

Fig. 6. Global blockchain creation through fog nodes as the distributed ledgers.

After that, V_F stores transaction record (CTR) $\langle p_c, r_{cf}, hd_c, C_c^{rem}, t_c, \sigma_c, p_f, C_f^{rem}, B_{cf}^{fn}, t_f, \sigma_f \rangle$ and also sends it back to V_C. In the same way as V_F, the signature of this received transaction record will be checked by V_C. If it is correct, then this transaction record will be stored on the blockchain-based certified transaction record of the vehicles as depicted in Fig. 4. Otherwise, V_C will request another transaction record.

Later, those created both-signed-transaction-records will be submitted to FN whenever encountering fog node infrastructure. As for V_C, that transaction record will be used to get stored data back or trace of offloaded computation on V_F. As for V_F, it will be used to claim a reward for sharing computational resources with other vehicles.

2) Transaction Record Submission: While encountering a fog node, both V_C and V_F have to submit their transaction record CTR, CPC, and CSC to FN. Upon receiving the record, FN will check the certificate revocation list (CRL) and verify the content of that transaction record whether any malicious activities are conducted by those vehicles. As an example, some vehicles may not submit some part of transaction records, change rating value, modify stored data and/or computational trace, and any others. In case of detecting those violations, FN will give payoff to those adversaries.

To detect those mentioned violations, FN will check the validity of certificates and also the content of transaction records. As for checking transaction records, FN may find that V_C claims that it has a transaction with V_F on its transaction record. However, somehow V_F claims that it does not have a transaction with V_C. Following this contradictory transaction record, FN then will check the signature on those transaction records and will decide which vehicle has created the wrong transaction records.

As an example, a V_C claims a transaction with a V_F by submitting its CTR to the $FN1$ as given in Fig. 6. After receiving CTR, $FN1$ requests data synchronization among all FN in order to check the validity of those signatures by checking the CPC and CSC of vehicles V_C and V_F, e.g., which FN issued those certificates, whether they are revoked, etc. If those certificates are valid, then $FN1$ will verify the hash of the CTR, i.e., the digest of the transaction record by means of the one-way hash function. The hash verification will let the $FN1$ to realize if any data tampering occurs on the CTR. Eventually, $FN1$ can recognize which vehicle has submitted wrongful transaction records.

In addition, after checking the transaction record, FN will issue a new CPC, CSC, payoff, and also the currency for the following vehicular fog computing service transaction as given in Fig. 5. FN will also put the old CPC and CSC into CRL. Those certificates stay on CRL until the vehicle is detected to leave the rural area.

Upon receiving new CPC and CSC, vehicles will delete the previous transaction record in order to decrease storage usage of this application. As a consequence, this application will not burden the computational resource of the vehicles.

IV. Security Analysis

This section will elaborate on the security analysis of the transaction record in some circumstances. We consider that malicious vehicles can modify transaction records and eavesdrop on communication channels to trace a particular vehicle. Considering vehicular network constraints and also less number of vehicles in a rural area, we can imagine that in such a situation, adversaries are likely to launch the Sybil attack, i.e., an attack which is done by an entity that possesses multiple identities, either legitimate or fraudulent, as discussed in several previous works [22], [19].

The Sybil attack can vary from launching an attack for taking small advantage until creating damage to the system or threatening the safety of driver/passengers. As for gaining benefit, the adversary can impersonate other legal/authorized vehicles and manipulate reputations in order to receive vehicular FCS. This motive can also cause a malicious legal vehicle to decline other vehicle's contributions and conduct replay attacks in order to interfere with payment of vehicular FCS. As for creating damage to the system, malicious vehicles can conduct a man-in-the-middle attack in order to reveal the session key and modify other vehicle's data. In addition, traces of other vehicle's paths can be utilized by the adversary for target profiling prior to launching more devastating attacks.

Among several references mentioned in the related work, we select the five most related works, SNVC [28], SAROS [27], Dua *et al.* [25], Yao *et al.* [26], Yang *et al.* [35], which are considered

TABLE III
COMPARISON OF SECURITY ANALYSES OF OUR PROPOSED METHOD WITH RESPECT TO RELATED WORKS

Trust Models	A1	A2	A3	A4	A5
SNVC [28]	✓	×	×	×	×
SAROS [27]	×	×	×	×	×
Dua et al. [25]	✓	✓	×	✓	×
Yao et al. [26]	✓	✓	×	✓	×
Yang et al. [35]	✓	✓	✓	×	✓
Our	✓	✓	✓	✓	✓

A1: impersonation and insider attack;
A2: replay attack;
A3: denial of transaction record;
A4: inability to trace;
A5: manipulation of rating / reputation attack;
✓: resistant against attack / available property;
×: not resistant against attack / unavailable property.

to be similar and comparable to our proposed method. Therefore, to the best of our knowledge, it is sufficient to simply discuss security analysis with respect to the most related works as given in Table III.

A. Impersonation and Insider Attack

Suppose adversary A is a registered vehicle and also posses its own CPC and CSC. Due to the fact that A is also able to have transactions with other registered vehicles, then A is also able to possess CPC and also transaction record of other certain vehicles. Following those actions, A attempts to impersonate that vehicle by recalculating SK^A on the CSC of that attacked vehicle. In this case, SK^A is calculated by using a signature obtained from that transaction record and also a randomly selected generator. After that, A will send the CPC of certain vehicles together with modified CSC and also transaction record to obtain new CPC and CSC so that submitted CPC and CSC will be revoked by FN and become invalid.

However, note that the generator of those keys, PK and SK, are only known by FN. Thus it is computationally infeasible for A to recalculate the correct SK. As a consequence, FN will easily find that submitted CPC and CSC are invalid credentials. Thus, A cannot impersonate other vehicles in this system.

Regarding this attack, SAROS [27] will suffer from this attack due to only relying on the evaluation of reputation without authenticating entity and utilizing PKI. As for SNVC [28], Dua *et al.* [25], Yao *et al.* [26], and Yang *et al.* [35], they can protect their system and user against this attack because they run authentication of entities as their trust establishment method.

B. Replay Attack

Suppose adversary A is a greedy entity that wishes to double reward after assisting other vehicles by resubmitting its own CPC, CSC, and transaction record to FN. Upon receiving those certificates and transaction record, then FN will check at first the validity of those certificates. If those are valid certificates, then FN will also check the CRL to make sure that those certificates are not listed. However, due to the fact that CPC and CSC are always changed and also the old ones are put on CRL after being submitted, then FN will easily find that those old CPC and CSC are no more valid to be used. As a result, this system is resistant to replay attacks.

The situation can be different for the method that relies only on the evaluation of reputation, such as SAROS [27] and SNVC [28]. They suffer from this attack due to the unavailability of the timestamp on the message and also lack of authentication procedure. On the contrary, Dua *et al.* [25] and Yao *et al.* [26], and Yang *et al.* [35] are resistant to this attack due to applying timestamps on each authentication message protocol.

C. Denial of Transaction Record Attack

This attack is conducted by opportunistic V_C that only wants to exploit computational resources of other vehicles or malicious V_F that does not want to hand over stored data/computation trace to FN in order to steal important data / computational trace. After releasing the both-signed-transaction record, that vehicle deceives its pair by discarding that transaction record. As a result, that transaction record is not submitted to FN. However, due to signature usage on each transaction record, that attacker cannot deny and run from the responsibility of doing malicious activities. Moreover, that malicious activities will lead to a reduction of deposited money in order to pay compensation costs and also receiving a penalty from FN by decreasing the next currency usage for bidding with other vehicles in establishing fog computing service.

As for this attack, all the compared works cannot resist this attack due to the absence of blockchain-based transaction record except for Yang *et al.* [35]. Even though some works use PKI and signature, such as SNVC [28], Dua *et al.* [25], and Yao *et al.* [26], they still suffer against this attack without the existence of a chain of the mutually signed transaction record.

D. Inability to Trace

From the previous explanation, it is clear that this system issues different certificates after vehicles encounter FN on the network-supported village. As a result, new transaction records will use different valid signatures and, at the same time, will close the possibility to trace other vehicles.

In the point of view of this security property, Dua *et al.* [25] and Yao *et al.* [26] can guarantee this property due to being proven under the CK adversary model and also utilizing certificate revocation procedure. As for SAROS [27] and SNVC [28], the methods fail to protect the vehicle's trajectory due to the absence of a public/private key revocation procedure. Moreover, revoking certificates can degrade the evaluation of reputation because they will be acknowledged as a new entity without reputation and need to gain reputation through interactions with other entities. At last, Yang *et al.* [35] also fail to provide this property due to employing fixed identity/certificate all the time.

E. Manipulation of Rating / Reputation Attack

Prior to conducting vehicular FCS, an adversary need to declare its rating based on previous transactions and initially assigned by TA to another vehicle (either server or client). In order to gain trust from another vehicle, the adversary should

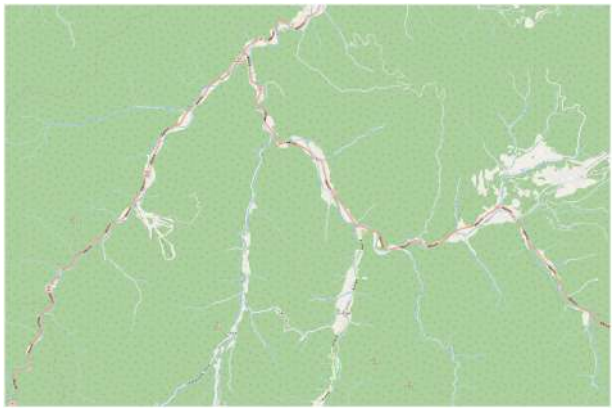

Fig. 7. Map of rural area in Fukushima prefecture, Japan.

show a good rating alongside the reasonable bidding price. However, blockchain-based transactions avoid the manipulation of rating attacks due to the existence of immutability property in the blockchain.

Similar to the previous analysis, the absence of blockchain-based transaction record causes all four compared works cannot resist this attack except for Yang *et al.* [35]. Even though SAROS [27] and SNVC [28] methods are based on evaluation of reputation, they still cannot resist this attack due to the lack of entities giving evaluations in order to form majority opinions. As a consequence, the node in SAROS and SNVC do not have any choice except to take only one rating opinion, which can lead to manipulation of rating/reputation attack.

V. Feasibility Analysis of BPT Scheme

This section presents the feasibility analysis of the BPT scheme considering the potency of vehicular FCS as given in simulation and also communication and computational cost as elaborated below. The potency of vehicular FCS is represented by the duration of communications and the number of communications among vehicles that possibly occur in a rural area. Intuitively, vehicular FCS can be realized if communication and computational costs are smaller than the length of communication between server and client vehicles. In addition, the number of communications among vehicles in a rural area indicates the capacity of vehicular FCS transactions approximately.

A. Simulation Results Using ONE Simulator

The simulation evaluates a rural area of Japan passed by road number 352, next to mount Aizu-Komagatake in Fukushima prefecture, as shown in Fig. 7. The map area is captured from the open street map, which is approximately about 336 km^2. Then it is converted into the wkt file by using QGIS Desktop 3.4.8 application prior to using it in ONE simulator [41].

We employ ONE simulator because the simulator enables source code integration between the network layer and application layer, in which the BPT scheme is executed, by using the Java programming language. Moreover, the simulator is designed to carry out the delay-tolerant-network (DTN) simulation, which is appropriate with our concept of temporarily store data into a server vehicle and finally submit data into a fog node (FN). Table IV shows the list of parameters used in this simulation.

TABLE IV
Parameters of Simulation

No	Parameters	Value
1	Approximate area	336 km^2
2	Vehicle speed	4 - 21 mps
3	Number of vehicles	10 - 40 vehicles
4	Communication range	up to 300 m (IEEE 802.11p)
5	Movement model	Car movement
6	Simulation running time	24 hours

As for approximately delivering real situations of rural areas, we investigate vehicle densities and vehicle speed as the input for the simulator. Considering the vehicle volume, a technical report from Washington State Transportation Center [42] tells that a rural area is divided into several classes with respect to the type of road and vehicle volume in a day. For example, some rural areas near urban areas exhibit a pattern similar to that of daily commuters in the urban area, but some other rural areas show quite different patterns. The pattern of daily commuters in the report comprises vehicle type, e.g., cars, trucks, motorcycles, etc., and vehicle volume. In addition, Ao *et al.* [43] also amplify the technical report by presenting an empirical analysis of household vehicle ownership of a new emerging rural area in the Sichuan Area. In [43], the average number of vehicles in a new emerging rural area varies from 0.13 to 0.54 per household. For example, a rural area with 100 households may have around 13 to 54 vehicles approximately. This number may increase or decrease depending on the social demography, e.g., type of work, place of work, family composition, etc., and also the class of rural area, e.g., interstate, remote, etc. As for the vehicle speed, we consider that the speed depends on the condition of the road and also the type of vehicle. For example, the speed of the car and trailer truck are different while passing through a rural area. Moreover, if the road surface or material is not good, the speed should be decreased due to safety regulations.

The simulation parameters in ONE simulator are set by referring to the IEEE 802.11p protocol as investigated in this work [44]. The communication range is defined as up to 300 meters. In order to capture the potency of vehicular FCS from vehicle commute in a rural area, we specify several parameters that can approximately characterize a rural area. Vehicle speed varies from 4 to 21 mps (meters per second), which is approximately equal to 15 to 75 kph (kilometers per hour), by following the car-based movement model. The number of vehicles is set to be 10–40 regardless of their movement direction.

In order to successfully perform vehicular FCS transactions in rural areas, there are two concerns that should be investigated, which are (1) how frequently having vehicular FCS and also (2) how long the duration of vehicular FCS transaction. Those two questions are revealed in this part by considering three important aspects that possibly exist in the implementation of the BPT scheme in a rural area. The parameters are (1) vehicle speed that depends on driver behavior, (2) number of vehicles that varies based on the daily commute of citizens, and (3) transmission

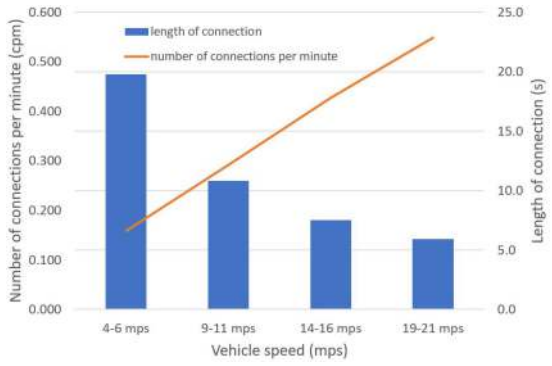

Fig. 8. Length of connection and number of connections per minute with respect to vehicle speed.

range that depends on path loss, characteristic of devices, and any other aspects. Thus, these results are expected to give the portrait of the potency of realizing the BPT scheme in a rural area, especially in the area of Japan, by following the parameters as described in Table IV.

Fig. 8 captures the effects of varying speed with respect to the number of connections maintained by two vehicles per minute and connection time between two vehicles. The result shows that increasing speed generates more encounters between two vehicles. As a consequence, it can lead to an increasing number of vehicular FCS transactions possibility in the rural area. As the opposite, increasing speed decreases the communication duration maintained between two vehicles. Thus, vehicle speed has to be considered with respect to the size of data sent in vehicular FCS transactions. The bigger the data are, the speed should be decreased in order to successfully establish vehicular FCS.

As for considering the length of the connection between two vehicles, there are three parameters that are investigated in this simulation, which are vehicle speed, number of vehicles, and transmission range. Fig. 9(a) shows that time to maintain the connection between two vehicles is influenced by the variation of speed usage, but not the number of vehicles. Intuitively it can be understood that communication between two vehicles occurs when two vehicles are within their each transmission range. As a result, by increasing the number of vehicles, it can only add the number of connections among all vehicles but not the connection period between two observed vehicles. Meanwhile, the transmission range influences the connection period between two vehicles, as shown in Fig. 9(b). It is also clear that the larger the transmission range, the longer the connection period maintained by two vehicles at the same speed. Fig. 9(c) also convinces us that the transmission range indeed affects the connection period between two vehicles, but not for the number of vehicles. Based on these findings, we can conclude here that in order to maintain reliable and longer vehicular FCS, vehicle speed and transmission range should be adjusted with the estimated time of vehicular FCS as elaborated in the following subsection.

As for the number of connections per minute, Fig. 10(a) tells that the number of vehicles in a rural area and vehicle speed also

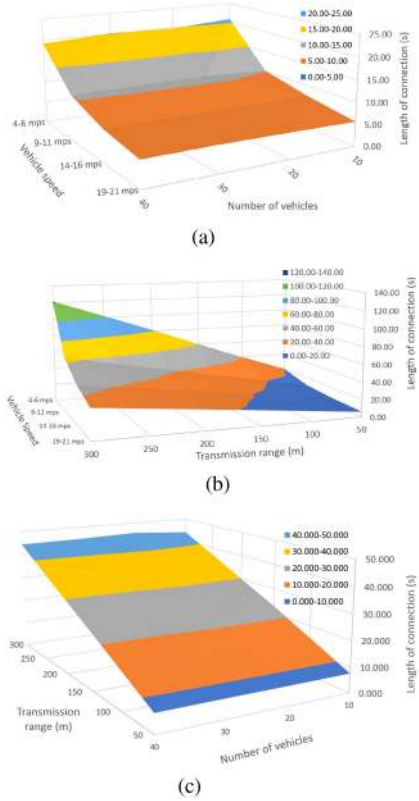

Fig. 9. Simulation result for connection time with respect to vehicle speed, number of vehicles, and transmission range. (a) Length of connection with respect to vehicle speed and number of vehicles. (b) Length of connection with respect to vehicle speed and transmission range. (c) Length of connection with respect to number of vehicles and transmission range.

contribute to the increasing number of connections between two vehicles per minute. It can be easily understood that the higher the speed, the bigger the chance to encounter more number of vehicles within the observed time. As a result, it can affect the number of transactions in a rural area. Unfortunately, the transmission range does not give impact to the number of transactions per minute, as shown in Fig. 10(b) that captures the number of transactions with respect to vehicle speed and transmission, and also Fig. 10(c) that captures the number of transactions with respect to the number of vehicles and transmission range as well.

B. Communication and Computational Cost Estimation

After revealing the potency of vehicular FCS transactions previously, this part adds up more considerations as the discussion material to capture the real situation of applying the BPT scheme in the rural area. As for investigating the feasibility issues, we consider a simple application of FCS that is data offloading. This application simply transfers some sensing data if the application detects running out of storage in some minutes/hours later in order to avoid overwriting of old data. Then, to answer the feasibility question, we have to reveal the real-time aspect by considering the computational and communication cost of the BPT scheme protocol, including data offloading from client

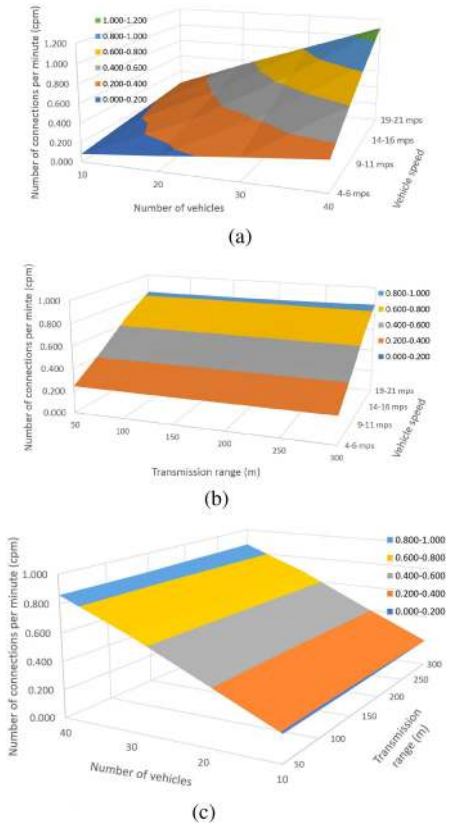

Fig. 10. Simulation result for number of connections per minute with respect to vehicle speed, number of vehicles, and transmission range. (a) Number of connections per minute with respect to vehicle speed and number of vehicles. (b) Number of connections per minute with respect to vehicle speed and transmission range. (c) Number of connections per minute with respect to number of vehicles and transmission range.

TABLE V
SYMBOLS USED IN THE COMMUNICATION AND COMPUTATIONAL COST DISCUSSION

Symbol	Description
d_t^{ee}	End-to-end delay
d_t^{oh}	Overhead delay
d_t^{od}	Offloaded data delay
L^{od}	Length of offloaded data
R^{od}	Bitrate of offloaded data
d_t^{bpt}	Computational delay of BPT scheme
d_t^{sv}	Computational delay of BPT scheme in server V_F side
d_t^{cl}	Computational delay of BPT scheme in client V_C side
L_i^{oh}	Length of message-i when transmitting BPT scheme protocol
R_i^{oh}	Bitrate of message-i when transmitting BPT scheme protocol
C_t^{te}	Cost for establishing trusted FCS in a rural area

vehicle to server vehicle within observation time. For increasing readability of the discussion, Table V explains symbols used in the discussion of the feasibility analysis

$$d_t^{ee} = d_t^{oh} + d_t^{od} \tag{7}$$

Equation (7) shows the calculation of end-to-end delay d_t^{ee} in executing BPT scheme by considering the factor of overhead delay d_t^{oh} of BPT scheme protocol and also delay d_t^{od} of data offloading from client vehicle to server vehicle at time t. From that equation, we can create new equations to give more insight

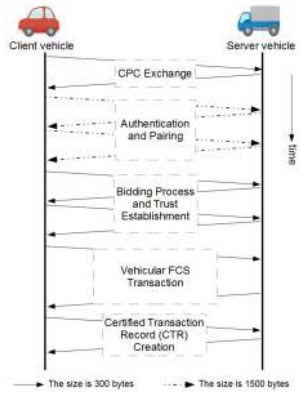

Fig. 11. Data flow of BPT scheme.

as given below.

$$d_t^{od} = \frac{L^{od}}{R^{od}}, \tag{8}$$

$$d_t^{oh} = \sum_{message} \frac{L_i^{oh}}{R_i^{oh}} + d_t^{bpt}, \tag{9}$$

$$d_t^{bpt} = d_t^{sv} + d_t^{cl}, \tag{10}$$

where L^{od}, R^{od}, L_i^{oh}, R_i^{oh}, d_t^{bpt}, d_t^{sv}, and d_t^{cl} are the length of offloaded data, bitrate of offloaded data, length of message i when transmitting BPT scheme protocol, bitrate of message i when transmitting BPT scheme protocol, computational delay of BPT scheme, computational delay of BPT scheme in server vehicle side, and computational delay of BPT scheme in client vehicle side respectively.

In addition, for giving a better understanding of these following equations, we need to provide data flow as given in Fig. 11. In that figure, all the parameters for calculating Equations (8) and (9) are visualized into message flows and computations on the vehicle's OBU. Then, the cost analysis is given as follows.

- For calculating delay d_t^{od} of data offloading in Equation (8) we need to know the transmission rate used in the transaction. We know that transmission rate R^{od} in IEEE 802.11p is not fixed. It can automatically change depending on distances, vehicle speeds, the presence of noise caused by nature or the existence of other communications within the same frequency and coverage, and any other factors. However, for simplifying analysis, we use 1 Mbps bitrate as discussed in [44]. As for offloaded data size, we use several data size scenarios, e.g., audio/video footage, the record of sensing information, etc., which are 5 Mb to 20 Mb.
- For calculating overhead delay d_t^{oh} of the transaction in Equation (9), we not only consider the size of data but also have to include the number of message flows as visualized in Fig. 11. In addition, we have to consider the computational delay d_t^{bpt} of the BPT scheme both in client vehicle d_t^{cl} and server vehicle d_t^{sv} as described further in Equation (10). For simplifying communication cost, we assume the size of each message is equal to 300 bytes for all messages except for both authentication and pairing

TABLE VI
END TO END DELAY CALCULATIONS AND TRUST ESTABLISHMENT COST OF BPT SCHEME AND DATA OFFLOADING

L^{od} (Mb)	d_t^{od}(s)	d_t^{oh}(s)	d_t^{ee}(s)	C_t^{te} (%)
5	5.00	2.472	7.472	33.08
10	10.00	2.472	12.472	19.82
15	15.00	2.472	17.472	14.15
20	20.00	2.472	22.472	11.00

parts, which are 1500 bytes. For both messages (300 bytes and 1500 bytes), they consist of 26 bytes overheads and payloads, including the BPT scheme protocol message and zero paddings, which are based on Ethernet frame. As for computational cost estimation, we cannot rely on ONE simulator because the simulator is not designed to calculate the computational cost of the application layer. Thus, for estimating the computational cost, we execute our protocol on a testbed based on the raspberry pi 3 model b+ with SD Card 16 GB and Raspbian Buster. The computational delay d_t^{bpt} of our BPT scheme, which is 2.405 seconds, is generated from java source code and executed 1000 times as a JAR application through command prompt by using OpenJDK 12. By considering the number of BPT scheme messages as given in Fig. 11 and also the experimental analysis regarding the average bitrate of communication as discussed in [44], the delay of BPT scheme including computational and communication cost in seconds is given in Equation (11).

$$d_t^{oh} = \frac{67.2\,\text{kbits}}{1000\,\text{kbps}} + 2.405\ \text{s} = 2.472\ \text{s} \tag{11}$$

Then considering the defined computational and communication costs, we can show Table VI to estimate the total end-to-end delay d_t^{ee} of vehicular FCS. It is clear that the BPT scheme protocol cost d_t^{oh} is smaller in comparison with the cost of data offloading d_t^{od} that varies from 5 to 20 seconds with respect to data size. By combining the BPT scheme protocol cost d_t^{oh} and data offloading cost d_t^{od}, we get a range of end-to-end delay from 7.472 to 22.472 seconds. By considering the comparison between the BPT scheme protocol cost d_t^{oh} and the total delay d_t^{ee}, Equation (12) is given for calculating cost C_t^{te} of establishing trusted FCS in the rural area in each offloaded data with the amount of 5 Mb, 10 Mb, 15 Mb, and 20 Mb.

$$C_t^{te} = \frac{d_t^{oh}}{d_t^{ee}} \times 100\% \tag{12}$$

C. Comparison of Communication and Computational Cost

Among five most related works, SNVC [28], SAROS [27], Dua *et al.* [25], Yao *et al.* [26], Yang *et al.* [35], and due to limited information about the detail of protocol, the size of a message, the cryptographic function, and any other tasks that can affect the costs, we unfortunately abandon to compare SAROS [27] and Yang *et al.* [35] with our scheme. Even though SNVC [28] does not explicitly provide the detailed cryptographic functions and the size of messages, we decide to include their work in this analysis by reconstructing their algorithm in the same programming language as used in this BPT scheme simulation. As for the size of messages, we approximately compute their message format based on the ECC algorithm defined in the IEEE 1609.2 standard, which specifies the use of SHA-256 message-digest algorithm, the curve type of secp256r1, and the ECC-256 b. Regarding the standard of IEEE 1609.2 and the SNVC algorithm, we construct the component of a cryptographic message sent by a vehicle based on X.509 format (for the public key) and PKCS8 (for the private key) provided by the oracle java.security.spec. library package as follows.

- Vehicle certificate, including vehicle identification number (17 bytes), vehicle public key based on X509 format (91 bytes), a certification authority (CA) signature-based on SHA-256 with ECDSA (71 bytes), own-signature based on SHA-256 with ECDSA (71 bytes).
- Message content, including other vehicle certificates (250 bytes) for introducing other vehicles, i.e., friend, friend of friend, friend by reputation, reputation value using (2 bytes) integer, and signature of the message content signed by the vehicle (71 bytes).

By considering the 1 Mbps bitrate of VANET and the total size of messages exchanged by two vehicles in a transaction, we finally obtain the communication cost of the SNVC method below.

$$\text{Comm. Cost SNVC} = \frac{2 \times 573\ \text{bytes}}{1000\,\text{kbps}} = 0.009\ \text{s}. \tag{13}$$

For deriving computational cost, we run the SNVC method on the same raspberry-pi platform as our work with 1000 times repetitions and OpenJDK12. The experiment generates the average computational cost of the SNVC method around 14.156 ms. As for the remaining works, Dua *et al.* [25], Yao *et al.* [26], they explicitly describe the detailed protocol and also the analysis of each protocol in the point of view of communication and computational cost. As a result, we can compile the comparison of communication and computational cost, as presented in Table VII.

TABLE VII
COMPARISON OF COMMUNICATION AND COMPUTATIONAL COST

Trust model	Comm. cost (s)	Comp. cost (s)	d_t^{ee}(s)
Dua et. al [25]	0.003	0.1406	5.1436
Yao et. al [26]	0.070	1.2430	6.3130
SNVC [28]	0.009	0.0142	5.0232
Our	0.067	2.4050	7.4720

Table VII shows that our proposed method is the most expensive cost among other methods. It is expected because our method is more complex with respect to the other three methods which consists of authentication and pairing, bidding price and rating exchange, trust computation, and also generating blockchain-based transaction record. The work of SNVC [28] is the most lightweight approach due to using simple messages and certificates exchange among vehicles for establishing trust based

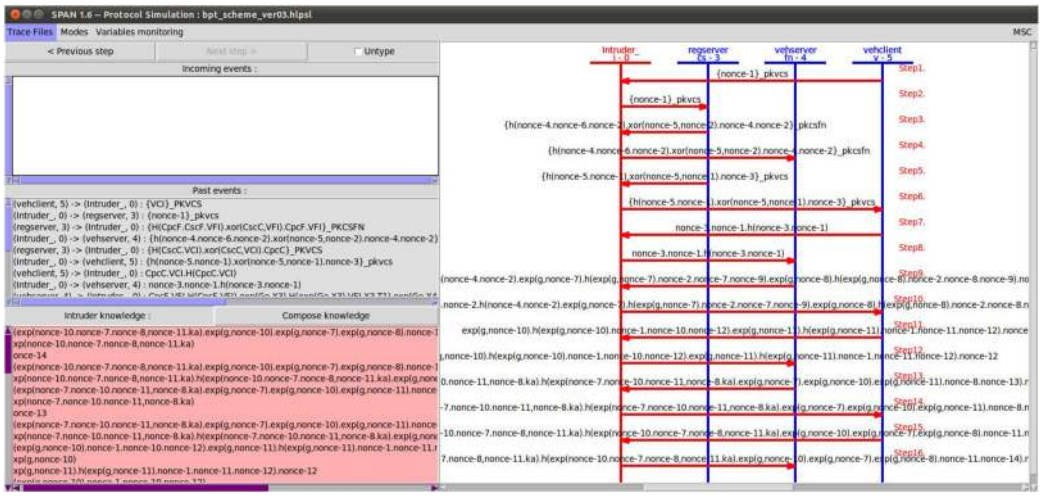

Fig. 12. Visualization of attacks on the BPT scheme using SPAN+AVISPA.

on friendship graph. However, their method is not appropriate in the rural situation with less number of vehicles because they need to communicate with a lot of vehicles for establishing a valid reputation table based on the social network approach. Moreover, the SNVC method is vulnerable against several known attacks in vehicular network elaborated in Section IV.

Dua *et al.* [25] show that their method is more lightweight with respect to our method and Yao *et al.* [26] but heavier with respect to SNVC [28]. It is not surprising because they employ Diffie-Hellman-based Elliptic Curve Cryptography for authenticating entities and creating a session key, in which the computational cost is heavier than the computational cost of simple messages and certificate exchanges as done in SNVC [28]. However, due to the absence of a vehicular evaluation system which we consider necessary for vehicular FCS as mentioned in Section II-A, their method suffers from several known attacks as discussed in Section IV. At last, Yao *et al.* [26] are more expensive than Dua *et al.* [25] and SNVC [28] because they employ three entities in establishing trusted vehicular FCS and also utilize RSA 1024 bits encryption, which indeed contributes to the increase of communication and computation cost. Even though Yao *et al.* [26] are more expensive, their work is not fit the environment of a rural area due to the need to connect to network infrastructures prior to establishing vehicular FCS.

D. Simulation Result Using AVISPA

As for security analysis, we employ the widely known tools for security analysis in the industry called Avispa (Automated Validation of Internet Security Protocols and Applications) [45]. The attack visualization as given in Fig. 12 is done by using SPAN, i.e., a Security Protocol ANimator for AVISPA, which is developed and demonstrated by a group of researchers and practitioners [46], [47]. The aim of this simulation is to investigate the security of our BPT scheme against replay attack and man-in-the-middle (MITM) attack. In order to do that, at first, we expose our BPT scheme agents to the intruder, as depicted in Fig. 12. Then, we utilize the CL-Atse (Constraint Logic-based

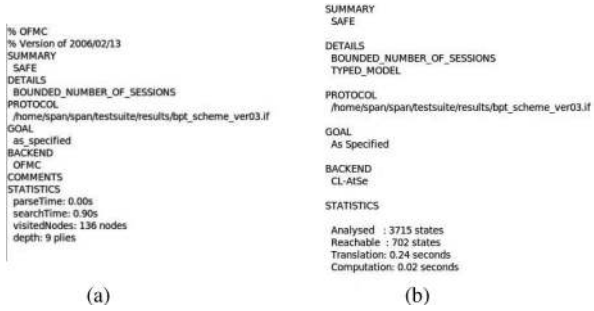

Fig. 13. Simulation results in the case of replay attack and man in the middle attack. (a) The result of OFMC backend for our BPT scheme. (b) The result of CL-Atse backend for our BPT scheme.

Attack and Searcher) and OFMC (on-the-fly-model-checker) backend for automatically analyzing and generating a report of the experiment.

The OFMC and CL-Atse backends basically execute the BPT scheme by applying the Dolev-Yao (DY) model. As a consequence, the intruder can simply collect any exchanged messages among the agents even though the messages are encrypted. By using the properties of the DY model, those backends investigate whether the intruder can reveal any secret parameters used for creating session key / secure communication channels in vehicular FCS. In case of finding potential attacks, the backends show attack traces in the reports which demonstrate the flow of some messages and what benefits that the intruder can gain from the attacks.

The analysis of OFMC and CL-Atse backends are presented in Fig. 13. As for the replay attack, the backends investigate whether the intruder can run the BPT scheme by replaying the collected messages. As for the MITM attack, the backends search any possibility to break the system, e.g., impersonating the agents, revealing secret information, etc., thoroughly by feeding the intruder with some pieces of knowledge of the normal session of BPT scheme. Based on the results, we believe

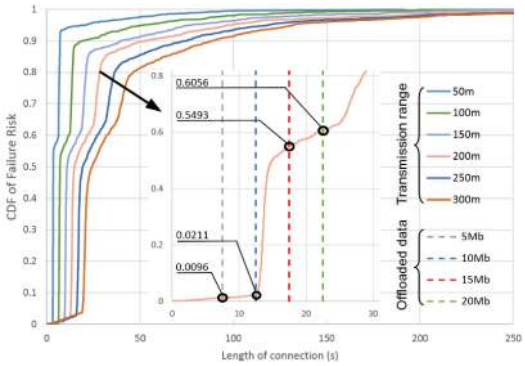

Fig. 14. CDF versus length of communication between server and client vehicles with speed 14–16 mps and 200 meters transmission range considering 5 Mb, 10 Mb, 15 Mb, and 20 Mb data offloading.

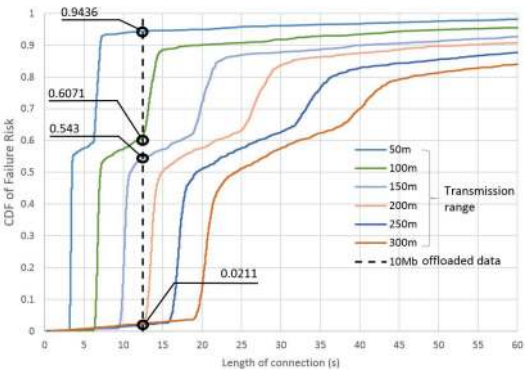

Fig. 15. CDF versus length of communication between server and client vehicles with speed 14–16 mps considering 10 Mb data offloading.

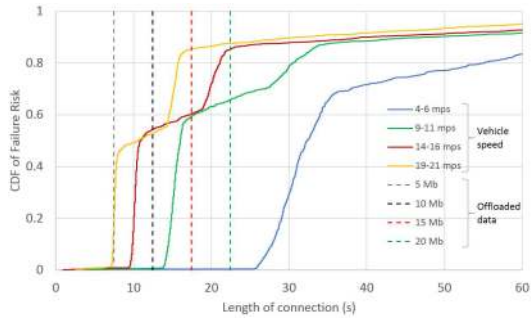

Fig. 16. CDF versus length of communication between server and client vehicles with 150 *m* transmission range considering 5–20 Mb data offloading.

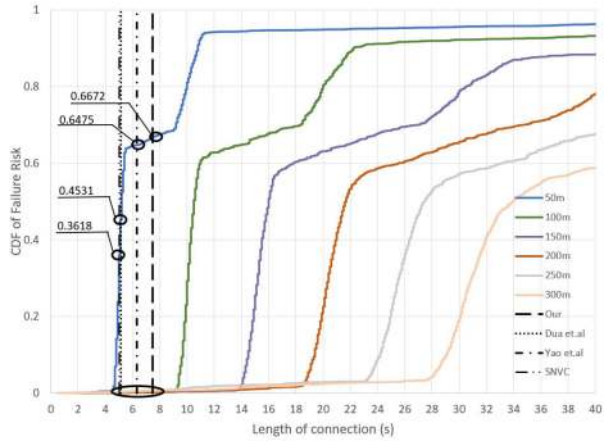

Fig. 17. Comparison of CDF versus length of communication between server and client vehicles with respect to Dua *et al.* [25], Yao *et al.* [26], and SNVC [28] considering 5 Mb data offloading.

that our BPT scheme is proven to be secure against the replay attack and MITM attack.

E. Feasibility Analysis

In order to conduct feasibility analysis, we use cumulative distribution function (CDF) for the assessment of failure risk conducting the BPT scheme, including data offloading in a rural area of Japan. In addition, based on the simulation results shown in the previous subsection, we narrow down investigation parameters into vehicle speed and transmission range in order to infer feasibility analysis. As a sample, in Fig. 14, we show the risk for the scenario of 10 vehicles moving with the speed of 14–16 mps by using the transmission range of 50–300 meters.

Based on Table VI, we set the end-to-end delay to 7.472 seconds, 12.472 seconds, 17.472 seconds, and 22.472 seconds, i.e., correlating to data offloading 5 Mb, 10 Mb, 15 Mb, 20 Mb, respectively, in order to show the risk of each transmission range usage. As a result, the increase of communication time between server and client vehicles affects the risks of failure, which are 0.96%, 2.11%, 54.93%, and 60.56% in 200 meters transmission range for 5 Mb, 10 Mb, 15 Mb, and 20 Mb data offloading respectively. In another case, Fig. 15 exposes that decreasing transmission range can degrade the probability of successful transactions. As for 200 meters, 250 meters, and 300 meters transmission ranges usage, the risks are almost equal to around 2.1%. The rest of the risks are 54.3%, 60.71%, and 94.36% for transmission range 150 meters, 100 meters, and 50 meters, respectively.

In Fig. 16, we present CDF with a different focus to show the impact of vehicle speed with respect to failure risk considering 150 *m* transmission range usage. For all offloaded data sizes, the risk for the speed of 4–6 mps is stable at around 0.4%. However, for other speed options, the risks dramatically increase when the length of connection is bigger than 12.472 *s* and 7.472 *s* for the speed 9–11 mps and the speed 14–16 mps, respectively. As for the speed 19–21 mps, it can be seen that the risk steeply increases right before the line of end-to-end delay 7.472 *s*, which makes the speed of 14–16 mps and 150 *m* transmission range usages are not the appropriate option for any offloaded data size in Fig. 16.

By using Table VII, we present the comparison of our BPT scheme with respect to the most similar related work that can be analyzed here. Similar to the previous graph, the end-to-end delays are set to be 5.0232 seconds, 5.1436 seconds, 6.3130 seconds, and 7.4720 seconds, which correspond to SNVC [28], Dua *et al.* [25], Yao *et al.* [26], and our work in 5 Mb data offloading scenario respectively. Then, the risk of failure in this scenario is presented in Fig. 17. Even though SNVC [28], Dua *et al.* [25], and Yao *et al.* [26] slightly outperform our BPT

TABLE VIII
RECAPITULATION OF FEASIBILITY STUDY FOR APPLYING BPT SCHEME

Range (m)	Feasibility (4 - 6 *mps*)				Feasibility (9 - 11 *mps*)				Feasibility (14 - 16 *mps*)				Feasibility (19 - 21 *mps*)			
	C1	C2	C3	C4	C1	C2	C3	C4	C1	C2	C3	C4	C1	C2	C3	C4
Our work																
50	◯	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
100	◯	◯	◯	×	◯	×	×	×	×	×	×	×	×	×	×	×
150	◯	◯	◯	◯	◯	◯	×	×	◯	×	×	×	Δ	×	×	×
200	◯	◯	◯	◯	◯	◯	◯	×	◯	◯	×	×	◯	Δ	×	×
250	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Δ	×	◯	Δ	Δ	×
300	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Δ	◯	◯	Δ	×
Dua et al. [25]																
50	◯	Δ	×	×	Δ	×	×	×	×	×	×	×	×	×	×	×
100	◯	◯	◯	Δ	◯	Δ	×	×	◯	×	×	×	Δ	×	×	×
150	◯	◯	◯	◯	◯	◯	Δ	×	◯	Δ	×	×	◯	Δ	×	×
200	◯	◯	◯	◯	◯	◯	◯	Δ	◯	◯	×	×	◯	Δ	×	×
250	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	×	◯	◯	Δ	×
300	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Δ	◯	◯	Δ	Δ
Yao et al. [26]																
50	◯	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
100	◯	◯	◯	×	◯	×	×	×	◯	×	×	×	Δ	×	×	×
150	◯	◯	◯	◯	◯	◯	×	×	◯	×	×	×	◯	×	×	×
200	◯	◯	◯	◯	◯	◯	◯	Δ	◯	◯	×	×	◯	Δ	×	×
250	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Δ	×	◯	◯	Δ	×
300	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Δ	◯	◯	Δ	Δ
SNVC [28]																
50	◯	Δ	×	×	Δ	×	×	×	×	×	×	×	×	×	×	×
100	◯	◯	◯	Δ	◯	Δ	×	×	◯	×	×	×	Δ	×	×	×
150	◯	◯	◯	◯	◯	◯	Δ	×	◯	Δ	×	×	◯	Δ	×	×
200	◯	◯	◯	◯	◯	◯	◯	Δ	◯	◯	×	×	◯	Δ	×	×
250	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	×	◯	◯	Δ	×
300	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	Δ	◯	◯	Δ	Δ

C1, C2, C3, C4: End-to-end delay $d_t^{e^e}$ corresponding to 5 Mb, 10 Mb, 15 Mb, 20 Mb data offloading respectively; ◯: High Feasibility; Δ: Low Feasibility; ×: No Feasibility.

scheme, we can see that the failure risk of ours and the other related works are almost similar with respect to 100 meters until 300 meters transmission range. The differences in that figure are clearly seen for only the failure risks in 50 meters transmission range parameter, which are 0.3618, 0.4531, 0.6475, and 0.6672, for SNVC [28], Dua *et al.* [25], Yao *et al.* [26], and our work respectively.

In order to simplify the results of failure risk as given in Fig. 14, Fig. 15, and Fig. 16, we classify the feasibility of applying the BPT scheme and data offloading into three criteria, i.e., high feasibility, low feasibility, and no feasibility. High feasibility criterion means that the BPT scheme transaction, including data offloading, is naturally feasible in the defined vehicle speed, transmission range, and size of offloaded data. Low feasibility criterion means that the transaction is possibly failed, and as a consequence, it needs more actions, e.g., transmission range adjustment and vehicle movement synchronization, in order to successfully conduct the BPT scheme. We will leave the discussion of enhancing BPT scheme performance in low feasibility criterion for future work. As for no feasibility criterion, it is not recommended to perform the BPT scheme under this criteria. The criteria of high feasibility, low feasibility, and no feasibility are determined as follows

$$\mathcal{F} = \begin{cases} H, & \text{if } 0\% \leq \mathcal{R} \leq 5\% \\ L, & \text{if } 5\% < \mathcal{R} \leq 50\% \\ N, & \text{if } \mathcal{R} > 50\% \end{cases}$$

where $\mathcal{F}$, $\mathcal{R}$, H, L, and N are feasibility, failure risk, high feasibility, low feasibility, and no feasibility, respectively. For giving more comprehensive results, Table VIII recapitulates the feasibility analysis of the BPT scheme, including data offloading for each option of transmission range, vehicle speed, and size of offloaded data.

Based on Table VIII, we can see that almost in all vehicle speeds and data offloading options, utilizing 300 meters transmission range can result in high feasibility of FCS transaction, except for vehicle speed 14–16 mps in 20 Mb data offloading and also vehicle speed 19–21 mps in 15 Mb and 20 Mb data offloading. In another case, moving at the lowest speed can also achieve high feasibility of FCS transaction for all data offloading except for 10 Mb and 15 Mb data offloading in 50 meters transmission range, and also 20 Mb data offloading in 50 meters and 100 meters transmission range.

Regarding the feasibility analysis result of Dua *et al.* [25], Yao *et al.* [26] and SNVC [28], we can see that the results are almost similar in all transmission range and vehicle speed. Minor differences can be seen in a way that our result shows no feasibility, but two other works show low feasibility or high feasibility. However, we consider the differences are not significant in comparison with overall feasibility results. Moreover, considering security and feasibility analyses, we can argue that our achievements outperform other work because we can provide more secure vehicular FCS in a rural area just by insignificantly sacrificing the feasibility with respect to other related work.

As a summary, data offloading size should be considered at the beginning of the BPT scheme for carrying trusted and feasible FCS transactions. Thus, for maximizing the feasibility of FCS transactions in the BPT scheme, the client and server vehicles should synchronize both speed and transmission range based on

their data offloading size. For example, in the bidding process and trust establishment, client vehicles can propose speed and transmission range adjustment to accommodate bigger data offloading and faster bitrate. To attract server vehicle participation in FCS transactions, server vehicles can receive more currencies or compensations from the FCS transactions if they accept client vehicle proposals for speed and transmission range adjustments. However, using a wider transmission range for maintaining longer communication time between server and client vehicles can cause battery drains faster. Furthermore, for some places driving at a very slow speed can endanger the safety of drivers and passengers due to some criminal actions.

VI. Conclusion and Future Work

A rural area can disturb FCS transactions due to the limited number of network infrastructures. In order to enable trusted vehicular FCS transactions in the rural area, we proposed the BPT scheme in this paper. BPT scheme establishes trust between server vehicle and client vehicle based on local and global trust computation. Local trust enables vehicle FCS by considering incentive value, ability to authenticate, and trust computation. Meanwhile, global trust determines rewards and punishments for each vehicle based on the certified transaction record in order to eliminate the number of attacks or malicious activities.

Simulation results show that vehicular communication in a rural area is influenced by three factors, which are vehicle speed, transmission range, and the number of vehicles. As for determining the length of connection, users need to adjust vehicle speed and transmission range. In another case, the number of connections is mostly determined by vehicle speed and the number of vehicles. The security analyses against possible attacks in the rural area demonstrate that our method can outperform the most related works. Then, feasibility analysis by considering failure risk shows that our method scheme is highly feasible to be realized in the rural area even though in some minor criteria of vehicle speed, transmission range and offloaded data, our work is categorized as lower feasibility with respect to the most related works. However, those minor differences are insignificant considering the protection of our method against security issues/attacks that can possibly cause great losses to the users, vehicles, and the system of the vehicular network.

For future work, we will investigate vehicle speed and transmission range adjustment with respect to the size of offloaded data for enhancing the feasibility of the BPT scheme transactions. In addition, the authentication and pairing parts tend to cause higher computational cost due to the use of the huge size of integers. As a consequence, those parts will be redesigned to accommodate lower end-to-end latency.

Acknowledgment

Authors thank to several unknown reviewers and colleagues who share their thought to increase the quality of this paper.

References

[1] O. Consortium, "Openfog reference architecture for fog computing," OpenFog consortium, Tech. Rep. OPFRA001.020817, 2017. [Online]. Available: http://site.ieee.org/denver-com/files/2017/06/OpenFog_Reference_Architecture_2_09_17-FINAL-1.pdf

[2] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.

[3] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, Jan. 2017.

[4] W. Hu, Z. Feng, Z. Chen, J. Harkes, P. Pillai, and M. Satyanarayanan, "Live synthesis of vehicle-sourced data over 4G lte," in *Proc. 20th ACM Int. Conf. Modelling, Anal. Simul. Wireless Mobile Syst.,* New York, NY, USA: ACM, 2017, pp. 161–170.

[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 Trans. Veh. Technol.*, vol. 65, no. 6, pp. 3860–3873, Jun. 2016.

[6] F. Yang, J. Li, T. Lei, and S. Wang, "Architecture and key technologies for internet of vehicles: A survey," *J. Commun. Inf. Netw.*, vol. 2, no. 2, pp. 1–17, Jun. 2017.

[7] E. Ndashimye, S. K. Ray, N. I. Sarkar, and J. A. Gutierrez, "Vehicle-to-infrastructure communication over multi-tier heterogeneous networks: A survey," *Comput. Netw.*, vol. 112, pp. 144–166, 2017.

[8] M. Mouton, G. Castignani, R. Frank, and T. Engel, "Enabling vehicular mobility in city-wide ieee 802.11 networks through predictive handovers," *Veh. Commun.*, vol. 2, no. 2, pp. 59–69, 2015.

[9] A. Boukerche and R. E. D. Grande, "Vehicular cloud computing: Architectures, applications, and mobility," *Comput. Netw.*, vol. 135, pp. 171 – 189, 2018.

[10] 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.

[11] J. K. Fendji and J. Nlong, "Rural wireless mesh network: A design methodology," *Int. J. Commun., Netw. Syst. Sci.*, vol. 8, pp. 1–9, 2015.

[12] 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 *Proc. 2nd Int. Conf. Adv. Elect. Eng.*, Dec. 2013, pp. 277–281.

[13] Y. Sun and N. Zhang, "A resource-sharing model based on a repeated game in fog computing," *Saudi J. Biol. Sci.*, vol. 24, no. 3, pp. 687–694, 2017.

[14] S. Schrecker *et al.*, Industrial Internet of Things Volume G4: Security Framework, vol. g4, ed., *Industrial Internet Consortium*, Sep. 2016. [Online]. Available: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

[15] C. Fernandez-Gago, F. Moyano, and J. Lopez, "Modelling trust dynamics in the internet of things," *Inf. Sci.*, vol. 396, pp. 72–82, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025517305364

[16] R. Sugumar, A. Rengarajan, and C. Jayakumar, "Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)," *Wireless Netw.*, vol. 24, no. 2, pp. 373–382, Feb. 2016.

[17] H. Rathore, V. Badarla, and G. K. J., "Sociopsychological trust model for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 62, pp. 75 – 87, 2016.

[18] J. Guo, I.-R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in Internet of Things systems," *Comput. Commun.*, vol. 97, pp. 1 – 14, 2017.

[19] 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 Netw. Appl.*, vol. 10, no. 2, pp. 305–314, Mar. 2017.

[20] N.-W. Lo and H.-C. Tsai, "A reputation system for traffic safety event on vehicular ad hoc networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, Dec. 2009, Art. no. 125348.

[21] B. Lee, E. Jeong, and I. Jung, "A DTSA (detection technique against a sybil attack) protocol using SKC (session key based certificate) on VANET," *Int. J. Secur. Its Appl.*, vol. 7, pp. 1–10, 2013.

[22] M. Al-Mutaz, L. Malott, and S. Chellappan, "Detecting sybil attacks in vehicular networks," *J. Trust Manage.*, vol. 1, no. 1, May 2014, doi: 10.1186/2196-064X-1-4.

[23] 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 *Proc. MILCOM IEEE Mil. Commun. Conf.*, Oct. 2009, pp. 1–7.
[24] C. Chen, X. Wang, W. Han, and B. Zang, "A robust detection of the sybil attack in urban VANETs," in *Proc. 29th IEEE Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2009, pp. 270–276.
[25] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4359–4373, May 2018.
[26] Y. Yao, X. Chang, J. Misic, and V. Misic, "Reliable and secure vehicular fog service provision," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 734–743, Feb. 2019.
[27] R.-I. Ciobanu, R.-C. Marin, C. Dobre, and V. Cristea, "Trust and reputation management for opportunistic dissemination," *Pervasive Mobile Comput.*, vol. 36, pp. 44 – 56, 2017.
[28] T. R. Oliveira, C. M. Silva, D. F. Macedo, and J. M. S. Nogueira, "SNVC: Social networks for vehicular certification," *Comput. Netw.*, vol. 111, pp. 129–140, 2016.
[29] T. D. Huynh, N. R. Jennings, and N. R. Shadbolt, "Certified reputation: How an agent can trust a stranger," in *Proc. 5th Int. Joint Conf. Auton. Agents Multiagent Syst.,* New York, NY, USA: ACM, 2006, pp. 1217–1224.
[30] Z. Liu, J. Ma, Z. Jiang, and Y. Miao, "LCT: A lightweight cross-domain trust model for the mobile distributed environment," *KSII Trans. Internet Inf. Syst.*, vol. 10, no. 2, pp. 914–934, 2016.
[31] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147 782–147795, 2019.
[32] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, and R. Chen, "Nutbaas: A blockchain-as-a-service platform," *IEEE Access*, vol. 7, pp. 134 422–134433, 2019.
[33] R. Shrestha and S. Y. Nam, "Regional blockchain for vehicular networks to prevent 51% attacks," *IEEE Access*, vol. 7, pp. 95 033–95045, 2019.
[34] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1972–1983, Mar. 2020.
[35] Y. Yang, L. Chou, C. Tseng, F. Tseng, and C. Liu, "Blockchain-based traffic event validation and trust verification for vanets," *IEEE Access*, vol. 7, pp. 30868–30877, 2019.
[36] Carry, "Connecting merchants consumers with blockchain," Tech. Rep., May 2018. [Online]. Available: https://carryprotocol.io/static/docs/Carry_protocol-white_paper(ENG).pdf
[37] F. Dewanta and M. Mambo, "A mutual authentication scheme for secure fog computing service handover in vehicular network environment," *IEEE Access*, vol. 7, pp. 103 095–103114, 2019.
[38] F. Dewanta and M. Mambo, "Bidding price-based transaction: Trust establishment for vehicular fog computing service in rural area," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Mar. 2019, pp. 882–887.
[39] M. Abdalla, F. Benhamouda, and P. MacKenzie, "Security of the j-pake password-authenticated key exchange protocol," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 571–587.
[40] 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
[41] A. Keränen, J. Ott, and T. Kärkkäinen, "The one simulator for DTN protocol evaluation," in *Proc. 2nd Int. Conf. Simul. Tools Techn.,* ICST, Brussels, Belgium, Belgium: ICST (Inst. Comput. Sci., Social-Inform. Telecommun. Eng., 2009, pp. 1–55.
[42] M. Hallenbeck, M. Rice, B. Smith, C. Cornell-Martinez, and J. Wilkinson, "Vehicle volume distributions by classification," Wahington State Transportation Center, Tech. Rep., Jul. 1997. [Online]. Available: https://depts.washington.edu/trac/bulkdisk/pdf/VVD_CLASS.pdf
[43] Y. Ao, C. Chen, D. Yang, and Y. Wang, "Relationship between rural built environment and household vehicle ownership: An empirical analysis in rural Sichuan, China," *Sustainability*, vol. 10, no. 5, May 2018, doi: 10.3390/su10051566.
[44] F. A. Teixeira, V. F. e Silva, J. L. Leoni, D. F. Macedo, and J. M. Nogueira, "Vehicular networks using the IEEE 802.11p standard: An experimental analysis," *Veh. Commun.*, vol. 1, no. 2, pp. 91–96, 2014.
[45] Avispa, "Automated validation of internet security protocols and applications," May 2018. [Online]. Available: http://www.avispa-project.org/
[46] O. Heen, T. Genet, S. Geller, and N. Prigent, "An industrial and academic joint experiment on automated verification of a security protocol," in *Proc. IFIP Netw. Workshop Mobile Netw. Secur.*, 2008, pp. 39–53.
[47] T. Genet, "A short span avispa tutorial," IRISA, Tech. Rep. hal-01213074v3, 2015. [Online]. Available: https://hal.inria.fr/hal-01213074v3

Favian Dewanta (Member, IEEE) received the B.Eng. degree in telecommunication engineering in 2009 from Telkom University, Kota Bandung, Indonesia, the M.Eng. degree in IT convergence engineering in 2013 from the Kumoh National Institute of Technology, Gumi, South Korea, and the Ph.D. degree in electrical engineering and computer science from Kanazawa University, Kanazawa, Japan, in 2019. He is currently an Assistant Professor with the School of Electrical Engineering, Telkom University. His research interests include authentication, trust establishment, information security, edge or fog computing, IoT, vehicular network, wireless sensor network, industrial network, and real-time system.

Masahiro Mambo (Member, IEEE) received the B.Eng. degree from Kanazawa University, Kanazawa, Japan, in 1988, and the M.S.Eng. and Dr.Eng. degrees in electronic engineering from the Tokyo Institute of Technology, Tokyo, Japan, in 1990 and 1993, respectively. In 2011, after working with the Japan Advanced Institute of Science and Technology, Tohoku University, Sendai, Japan, and the University of Tsukuba, Tsukuba, Japan, he joined Kanazawa University. He is currently a Professor with the Faculty of Electrical, Information and Communication Engineering, Institute of Science and Engineering. His research interests include information security, software protection, and privacy protection. He was the Co-Editor-In-Chief of the International Journal of Information Security, and the Steering Committee Chair of the International Conference on Information Security and the Chair of the Technical Committee on Information Security in Engineering Sciences Society of the Institute of Electronics, Information and Communication Engineers (ISEC in ESS of IEICE).