IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON D2D COMMUNICATIONS: SECURITY ISSUES AND RESOURCE ALLOCATION

Received February 1, 2019, accepted February 24, 2019, date of publication March 8, 2019, date of current version March 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2903202

Blockchain-Based Traffic Event Validation and Trust Verification for VANETs

YAO-TSUNG YANG[1], (Student Member, IEEE), LI-DER CHOU[1], (Member, IEEE), CHIA-WEI TSENG[1], (Student Member, IEEE), FAN-HSUN TSENG[2], (Member, IEEE), AND CHIEN-CHANG LIU[1]

[1]Department of Computer Science and Information Engineering, National Central University, Taoyuan 320, Taiwan
[2]Department of Technology Application and Human Resource Development, National Taiwan Normal University, Taipei 106, Taiwan

Corresponding author: Li-Der Chou (cld@csie.ncu.edu.tw)

This work was supported in part by the Ministry of Science and Technology (MOST), Taiwan, under Grant MOST 102-2221-E-008-039-MY3, Grant MOST 103-2221-E-008-090-MY3, Grant MOST 108-2623-E-008-004, and Grant MOST 108-2636-E-003-001.

ABSTRACT Sharing traffic information on the vehicular network can help in the implementation of intelligent traffic management, such as car accident warnings, road construction notices, and driver route changes to reduce traffic congestion earlier. In the future, in the case of autonomous driving, traffic information will be exchanged more frequently and more immediately. Once the exposed traffic incident is incorrect, the driving route will be misleading, and the driving response may be in danger. The blockchain ensures the correctness of data and tampers resistance in the consensus mechanism, which can solve such similar problems. This paper proposes a proof-of-event consensus concept applicable to vehicular networks rather than proof-of-work or proof-of-authority approaches. The traffic data are collected through the roadside units, and the passing vehicles will verify the correctness when receiving the event notification. In addition, a two-phase transaction on blockchain is introduced to send warning messages in appropriate regions and time periods. The simulation results show that the proposed mechanism can effectively feedback the correctness of traffic events and provide traceable events with trust verification.

INDEX TERMS Blockchain, event validation, proof-of-event consensus, trust verification, vehicular ad-hoc networks.

I. INTRODUCTION

With the maturity of dedicated short range communication (DSRC) radio technology, many vehicles-to-anything (V2X) applications are important drivers of intelligent transportation systems (ITSs). Vehicular ad hoc networks (VANETs) will be responsible for cooperating traffic data among on-board units (OBUs) equipped with vehicles through vehicle-to-vehicle (V2V) communication and collaborating between OBUs and roadside units (RSUs) through vehicles-to-infrastructure (V2I) communication. The sharing of such information is an important factor in driving navigation and safety applications, especially for the development of autonomous vehicles. When the accident occurs, whether the relevant information can be transmitted correctly and effectively is very important for the overall traffic safety [1]–[4].

The types of traffic events in VANETs can be classified into three categories. 1) The first category is the notification between vehicles, which can be divided into single-hop and multi-hop, depending on the number of vehicles transmitted and time to the scene of the event. In the application of single-hop, the road safety is mainly based on the passing time less than three seconds, such as emergency braking, lane changing, roadside parking and reversing; in multi-hop applications, it includes congestion notifications, emergency vehicle approaching, dangerous driving and traffic accidents. 2) The second category is the event notification from facilities, including road hazard, roadwork warning, traffic sign failure, road adhesion, visibility, and wind. 3) The third category is other events that can be collected from social media, such as parades, protests. In European Telecommunications Standards Institute (ETSI) standards, the data flow of primary road safety application is transmitted through Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DEMNs) [5], [6]. The former

The associate editor coordinating the review of this manuscript and approving it for publication was Vlad Popescu.

is mainly used for regular broadcast of vehicles within a single-hop range to exchange information such as vehicle presence, location and status; the latter can carry events via multi-hop ITS stations [7].

In terms of information security and privacy in VANETs, the following five major requirements must be met, including: 1) *Authentication*: Every identity must be guaranteed and verified. In addition, each valid message must be warranted. 2) *Integrity and correctness*: In the process of transmission, the data must be ensured that it is not modified or discarded, and the geographic data of the sender must be accurate to avoid the receiver being misled. 3) *Non-repudiation*: The sender cannot deny the operation of the data. 4) *Privacy*: The true identity cannot be linked through the data directly and with a certain degree of anonymity; and 5) *Efficiency*: Under the above conditions, a certain real-time guarantee must be reached [8], [9].

Although the public key infrastructure (PKI) based authentication protocol can isolate external attacks and maintain anonymity, it is difficult to defend against internal attacks, e.g., a selfish node forging a congestion event in an attempt to speed up a journey, or the central ITS station being taken over by hackers to pass global fake events, etc., so it is necessary to propose better countermeasures for trust verification [10]. The trustworthiness based on reputation systems to identify the falsification information have been proposed in some literatures, but relatively increases the amount of information exchanged in VANETs and also result in high transmission delay [11]–[13].

The blockchain is a decentralized technique that combines cryptography, digital signatures, hash functions, and time sequence. It has caught many attentions because of the popularity of *Bitcoin* and other digital currencies [14]. Each block chained like a chain contains the hash value of the previous block to ensure that the data on the chain are immutable. All historical transactions stored on the blockchain can be tracked and fast accessed by nodes of the network; moreover, maintaining the fairness and order of this decentralized ledger is the consensus algorithm. It can solve the consensus problem to decide who will get the right to submit a transaction to the database. The most common mechanisms include *Proof-of-Work* (PoW), *Proof-of-Stake* (PoS), *Proof-of-Authority* (PoA), *Practical Byzantine Fault Tolerance* (PBFT), etc. [15]–[17].

This paper proposes a traffic event validation and trust verification mechanism based on the decentralized nature of blockchain. The RSU first uses the cooperative traffic information from vehicles and initiates the proposed *Proof-of-Event* (PoE) consensus algorithm among passing vehicles once the collected data meets the corresponding threshold. If the result of PoE is confirmed to be an incident, the vehicles in the adjacent area are going to be notified through the broadcast from the RSU, and the event stored on the blockchain will be permanently retained for public access. The contribution of this work is as follows.

1) The paper proposes a Blockchain-based Traffic Event Validation (BTEV) framework which introduces PoE consensus mechanism to achieve the reliability of confirming the event occurrences. This framework can verify traffic incidents through vehicles near the RSU while accomplishing the role of event alert.
2) This PoE mechanism can also identify the selfish or malicious behaviors and prevent the spread of false traffic warning messages.
3) In the existing literature, blocks (or transactions) are broadcast to all possible nodes to synchronize at one time. However, we divide the transactions on blockchain into two consecutive stages, first synchronizing the local blockchain then synchronizing the global blockchain. This helps deliver the warning messages in the appropriate region and time.
4) Each event is stored as a *synopsis* in a hierarchical, chronological, and geographic structure, which is a well-design combination of Merkle tree and Prefix tree to improve the efficiency of transactions on blockchain.
5) The simulation results show that the PoE mechanism can reduce the spread of fake events from vehicles by adjusting the threshold of RSUs.
6) To the best of our knowledge, we believe we are the first paper using event validation as the consensus strategy on blockchain in VANETs.

The rest of this paper is organized as follows: Section II discusses related work. In Section III, the proposed mechanism is introduced. Section IV illustrates the experiment results. Section V is the discussion. Finally, Section VI concludes this work.

II. RELATED WORK

Based on the existing PKI-based authentication, this paper adds the function of event validation to compensate for internal vulnerabilities, combines the technology of blockchain to make events traceable, and builds the decentralized shared database for fast access. In this section, we provide an overview of security, privacy, trust model, blockchain, and consensus mechanisms in VANETs.

A. SECURITY AND PRIVACY IN VANETS

The PKI-based framework can provide the basic security services for VANETs. The IEEE 1609 Working Group has defined the IEEE 1609.x Protocol Stack, a.k.a. Wireless Access in Vehicular Environments (WAVE), and proposed two ways of cryptographically signing ITS messages: Kerberos-like and PKI-like token system [18]. The former is very efficient and less power consumption by using symmetric key operations, but the management of keys requires an always-on connection and greatly increases the message traffic which may cause congestion. The latter is slower and complex in the keys management, but the authorization system can continue to operate even when there is no access to infrastructure. Therefore, various elliptic curve digital signature

algorithms (ECDSA) of PKI are evaluated for signing and verifying ITS safety messages, such as CAM and DEMN.

This kind of solutions can achieve the mutual trust mechanism between vehicles and central ITS stations while avoiding both masquerade and impersonation attacks [19], [20]. Nevertheless, distributing revocation information may cause congestion. In [21], Salem *et al.* proposed a lightweight dynamic PKI-based key distribution protocol for VANETs. This protocol can reduce the revocation overhead and improve network utilization by sending the revocation message only to the vehicles that have a probability of communication with the revoked vehicle.

Privacy is also an import requirement in VANETs. Public key, as a pseudonym, can ensure the user's true identity is hidden from all other users. In addition, the number of concurrently available pseudonyms can be limited to avoid Sybil attacks, for example, only one key pair is valid at any given time [22]. However, such pseudonym without true user identity linkage make it more difficult to recognize and disable a misbehaving node.

B. TRUST MODELS IN VANETS

The trust model is a possible countermeasure to evaluate the legitimacy of anonymous node behavior. A maintenance system for the trustworthiness of vehicles or data is an inevitable unit to judge the processing behavior of received information [9]. To accept and forward such message if the source is considered fully reputable; to accept it but do not forward it when the sender is more or less trustworthy; to reject and drop the message if the source is not trustworthy enough.

In [11], Raya *et al.* have formulated a fast misbehavior detection system to exclude malicious vehicles by aggregating the multiple dimension of data frequently. In [12], Lo and Tsai proposed a reputation system which can provide accurate and reliable traffic events through the design of two adjusted threshold values. In [13], Gómez Mármol and Martínez Pérez presented a proposal to use a fuzzy set to classify the trust level of events according to the reputation score given by the recommendation from all possible hops and the infrastructure through RSUs. Because reputation scores are based on the data collected as much as possible through multiple hops, the drawbacks of these models are data sparsity and high transmission latency, especially the volatile data from vehicles in high speed or in low density area.

The possible countermeasures are 1) the threshold-based event validation where an event is considered valid if the number of reports exceeds a certain threshold, or 2) the validation of group certificates to increase the efficiency of the transmission and the trustworthiness of the data. In [23], Hsiao *et al.* designed a message exchange protocol enabling timely collection and distribution of multi-hop alerts. In both [24] and [25], group signature is used to ensure the privacy of vehicles and threshold authentication is used to check the trustworthiness of received messages.

C. BLOCKCHAIN AND CONSENSUS MECHANISMS IN VANETS

The blockchain technology can be used to generate value-added services in ITS with secure, distributed, anonymous, autonomous, and immutable records. In addition, based on the decentralized nature of blockchain, trust management or consensus mechanism can be performed between distributed RSUs, which can effectively avoid the problem of centralized authorization [26]–[28].

The main purpose of the consensus algorithm is to avoid the fraudulent transactions on blockchain, i.e. to deal with the problem of information synchronization under the decentralized architecture, and to solve the Byzantine problem at the same time [29]. The PoW approach relies on the high computing power to calculate a hash value less than or equal to the current target value for the block by finding a nonce through the brute-force search. The first winner can chain his/her block to the next in the blockchain. The PoS approach requires block producers to hold a stake. The owner with the most coins has the lowest difficulty to find a nonce to produce the next block. The PoA approach relies on identity as a stake, and only trusted nodes can join in a network as block producers. The blockchain created in this way is also a permissioned blockchain. Producers can be publicly assigned by a central entity, called *centralized PoA*, or voted by other nodes, called *decentralized PoA*. A special mention must be made of the Delegated Proof-of-Stake (DPoS) approach, only stake owners can be elected as block producers, but the real consensus happens on the distributed PoA level [30].

Most existing literature is based on PoW, PoS and PoA to implement a consensus process. In [28], Yang *et al.* proposed a decentralized trust management system that joins PoW and PoS consensus mechanisms. This design enables all RSUs to compete to add a trust block from which the trustworthiness of vehicles can be extracted. The more trust value the RSU collects, the easier it is for the RSU to find the nonce to generate the block. In [31], Lu *et al.* proposed a PKI-based reputation system to establish a privacy-preserving trust model for VANETs. Three different blockchains with the same PoA mechanism are used to evaluate the reputation of each vehicle, act as the public ledger for all issued certificates, and prove absent by checking the revocation list. In [32], Malik *et al.* proposed a framework for authentication and revocation of transactions that not only authenticates vehicles with mitigating dependency on a trusted authority but also speedily updates the status of revoked vehicles in the shared blockchain ledger with the PoA mechanism. In [33], Kang *et al.* proposed an enhanced DPoS consensus scheme with two-stage security enhancement solution. The first stage is to select miners by reputation based voting. The second stage is to incentivize standby miners to participate in block verification using contract theory.

Unlike traditional consensus mechanisms, we introduce the PoE concept to synchronize the synopsis of events in

local areas and accelerate the transaction procedure on the blockchain in VANETs.

III. PROPOSED FRAMEWORK

The main features of the proposed BTEV framework includes 1) PoE mechanism which is a two-pass validation for an unproven incident, 2) two-phase transaction for fast event notification and efficient blockchain access, 3) trust verification of RSUs. Our design goal is to meet the security, privacy, and trust requirements base on blockchain technology. This section details the function of the proposed framework.

A. ASSUMPTIONS

1) EVENT DETECTION

The data dictionary has been defined for ITS applications and facilities in ETSI and contains a wide range of traffic information [34]. However, some situations are difficult to verify through other vehicles or road facilities, especially when the vehicle is moving, e.g. the human problem in vehicles involved in traffic. Therefore, this paper only focus on the part that can be verified through vehicles or RSUs, for example, using the location and speed information to detect over speeding or emergency braking. As for how to verify the location and speed of the car, there have been many related studies [2], [3], [35], so the scope of this paper is not detailed. In addition, to validate an event requires a threshold number of alerts. In [23], a synopsis is used to define a set of warnings with respect to the event. The synopsis allows other vehicles to determine if the total number of alerts exceed the threshold, but here we change to decide by both vehicles and RSUs.

2) PKI SYSTEM

We assume a PKI-based model [22] exists in our framework. Each vehicle equips an OBU with tamper-proof key storage and secures the threshold-based validation result in periodically transmitted CAMs with a digital signature and certificate. RSUs collect traffic information from vehicles in the vicinity and broadcast the warning messages via DENMs once the event is valid. In addition, we assume the RSU here has the high computing power to create the block and maintain the blockchain with each other via a wired network. And multiple Certificate Authorities (CAs) issue and revoke certificates of vehicles or cooperate and cross-certify each other. The procedure can be referred to the identity authentication and fast revocation of [32]. Moreover, Law Enforcement Authority (LEA) is responsible for the linkage between the public key and true identity for misbehavior tracking. Finally, we also assume the majority of vehicles and RSUs in the network are honest.

B. PROOF-OF-EVENT

The vehicle information, such as heading, speed, location, etc., to be exchanged for cooperative awareness is packaged in the CAM. Each signed CAM is sent within a single-hop repeatedly after a back-off time 100 ms or met a set of changing conditions, and accepted by the receiver if the certificate is valid [5]. A DENM contains information related to a road hazard or an abnormal traffic conditions and is disseminated over a long distance through multi-hop transmission [6]. In the proposed BTEV, each CAM of vehicles is collected by the near RSUs and each DENM is produced by the RSU when the unproven event is need to be verified or proven event is triggered. In addition, the access of the blockchain service is via DENMs as well. The procedure of the RSU in this work is shown in Fig. 1.

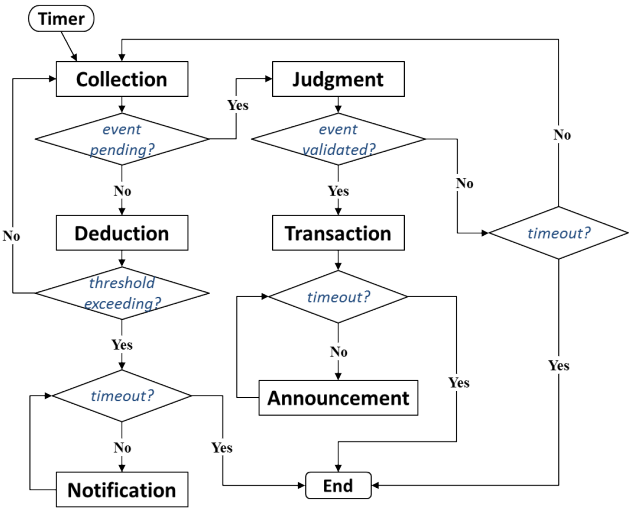


FIGURE 1. The flow chart of a RSU in BTEV.

PoE mechanism is a two-pass validation for an event. We suppose a synopsis $\mathbb{S}$ of an event E is a set of warning rules $\{W_1, W_2, \ldots, W_{|\mathbb{S}|}\}$. Both a vehicle and a RSU have a threshold-based event validation algorithm $G_V(\tau_v, m, \mathbb{S}, p_v)$. For a threshold τ_v and the number of rule matches m of $\mathbb{S}$ in a period time p_v, G_V will output 1 when $m \geq \tau_v$ and 0 when $m < \tau_v$. On the other hand, each RSU has another threshold-based event validation algorithm $G_R(\tau_r, k, \mathbb{S}, p_r)$. For a threshold τ_r and the number of rule matches k of $\mathbb{S}$ in a period time p_r where $p_r > p_v$, G_R will output 1 when $k \geq \tau_r$ and 0 when $k < \tau_r$.

In the first *Collection* phase, the RSU will collect traffic information via CAMs and get a snapshot $\mathbb{S}$ in a period of time. In *Deduction* phase, $(\tau_v, \mathbb{S}, p_v)$ will be generated if the RSU get the output 1 from G_V after unpacking the received CAMs. When the output is 1 and not expired, the RSU is going to *Notification* phase and broadcasts $(\tau_v, \mathbb{S}, p_v)$ via DENMs. Because the DENM is the multi-hop transmission, the range of verification can be extended. Therefore, in the second *Collection* phase, the RSU will be possible to collect more traffic information from the new coming vehicles. In addition, the result of G_V will be sent via the CAM with a signature S_c and a public-key certificate P_c of each vehicle to the RSU. If the output of G_V is found when p_v is expired and p_r is not expired, the RSU is going to *Judgment* phase. In this phase, the output of G_R will be calculated by

the RSU and the event will be confirmed if the output is 1. If the output is not 1 when p_r expired, the RSU will update or terminate the DENMs. After the event validated in this phase, the RSU will enter into *Transaction* phase and the event description will be put into the blockchain with the event evidence, the hash value of a combination of output signatures $\{S_c1, S_c2, \ldots, S_c|\tau_r|\}$ and certificates $\{P_c1, P_c2, \ldots, P_c|\tau_r|\}$ which belongs to the participated vehicles, then broadcasted to the vicinity via DENMs in multi-hop with geocasting in *Announce* phase. This two-pass validation mechanism is accomplished by a RSU and different vehicles through two different threshold-based validation algorithms. This PoE mechanism not only prevents the selfish or malicious vehicles from cheating, but also prevents RSUs from transmitting unverified or bogus event notification.

C. DATA STRUCTURE AND TRANSACTIONS

In *Transaction* phase, the RSU will submit the confirmed event to the blockchain. In order to make this process more efficient, we introduce a Merkle Patricia Trie (MPT) structure to the proposed framework [36]. In addition, we derive the idea from [37] but divide the transactions on blockchain into two consecutive stages based on the geographical regions, first synchronizing the local blockchain then synchronizing the global blockchain. This can help the delivery of the warning messages and the blockchain maintenance.

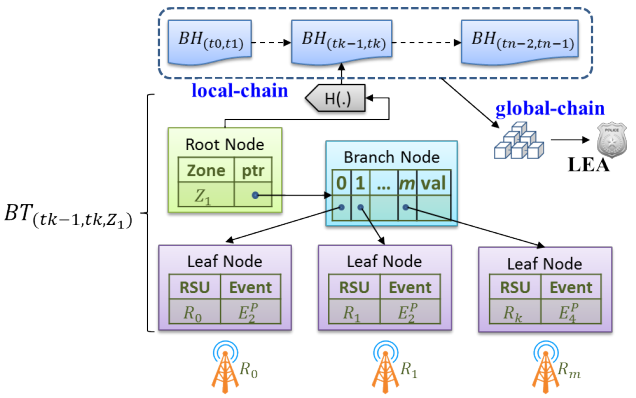


FIGURE 2. Data structure of the BTEV blockchain.

The data structure is illustrated with Fig. 2. This structure is an enhanced MPT, denoted BT, which is a mixture of Merkle trees and Prefix trees, designed specifically for our work in a chronological, geographical and hierarchical order. A leaf node in MPT records two items, one is the RSU id and the other is the event description. Each leaf node is indexed by a branch node. And the root node presents the zone of RSUs. All RSUs located in this zone can be indexed to the one of leaf nodes through the branch node. Each root node will be generated at the same time when the block is created. The block contains the header, denoted BH, a lifetime from t_{k-1} to t_k, and the root hash of the corresponding BT. The creator of new block is the first event announcer among RSUs in the same zone. When the new block is produced, the claimer must put its event evidence, the hash value of the combination of output signatures and certificates of participants, as the root hash for auditing and set the life time of the block, then broadcast to all RSUs in the same zone. That is, the block owner can be verified with its event evidence by every RSU in the same zone. All confirmed events during the new block lifetime will be recorded in the MPT associated with that block.

Each RSU only maintains the PoE operations for the blockchain belong to the same zone. This zone-based blockchain is called *local-chain* and only nodes in range can access it. The *local-chain* synchronization is to union MPT structures of coming events from different RSUs as shown in Fig. 3. Since each RSU has the designated leaf node, no events will be overwritten during this synchronization. But the event confirmed from the same RSU will be replaced with the new description. The number of times an event is logged can be adjusted by controlling the lifetime of the block.

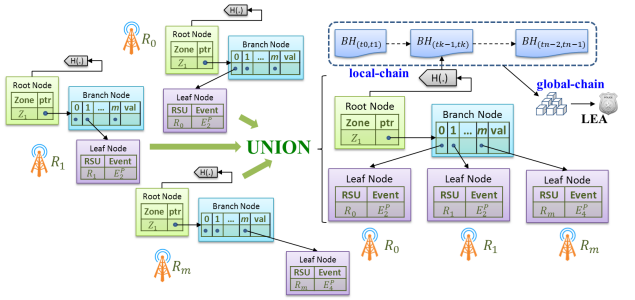


FIGURE 3. The union operation of MPT structures in local-chain.

In addition, for a long period time, e.g. one hour, the last block creator will be responsible for submitting the entire local-chain into the global blockchain, called *global-chain*, for public access. The *global-chain* consists of multiple *local-chains*; hence, the forking on the *global-chain* may occur. The solution is to compare the time offset. If there are multiple submitters to the *global-chain* at the same time, the winner will be the least offset from the first event validation time in the last block of its *local-chain* to the expiration time of the previous global block. After synchronization, this *global-chain* with all event descriptions will be permanently retained in LEA for further traffic adjudication.

D. TRUST VERIFICATION

For the event falsification, PoE can solve this kind of problem because each event is inspected through a threshold-based validation from different nodes with guarantees by their certificates. The false synopsis $\mathbb{S}$ in a CAM will always get the output 0 of G_V from other vehicles so the event is never triggered. If the false event description in DENM sent by a RSU, the received vehicle can verify its event evidence and report to the LEA directly if a bogus message found. Because this evidence verification takes more power consumption, the verifier is chosen randomly.

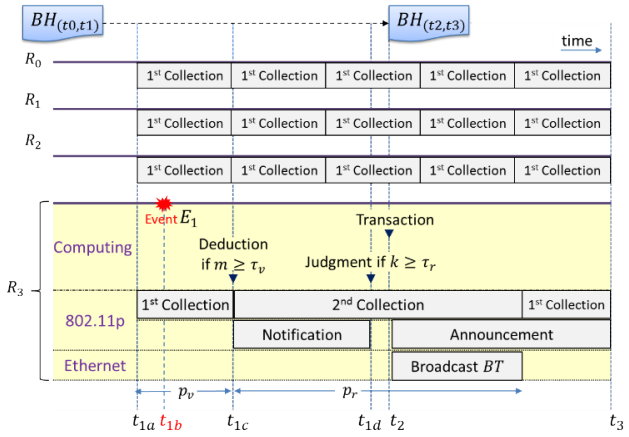


FIGURE 4. The scheduling of event validation on RSUs.

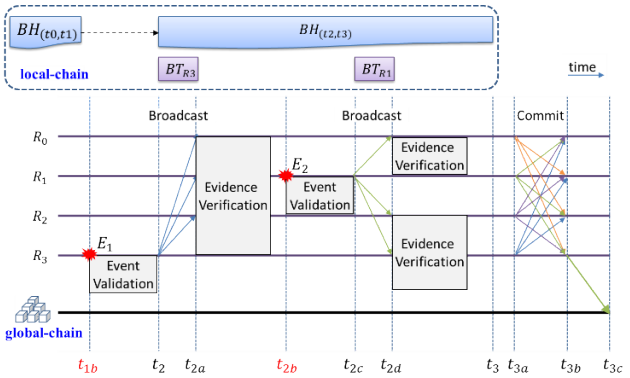


FIGURE 5. The procedure of PoE consensus mechanism.

When the last block creator prepares to submit the current *local-chain* to the *global-chain*, this creator will verify all the event descriptions with the provided evidences and calculate the corresponding hash value of each MPT in each block, then put these values with its signature to the pool. When the next block of global-chain is produced, the new block owner will verify all event descriptions and corresponding hash values of MPTs. If any failure in verification, the event description will be dropped and new hash value of MPT will be recalculated. This ensure all confirmed events can be recorded in the blockchain.

E. A SCENARIO

All RSUs in the same zone are connected to each other via Ethernet and communicate with the vehicle via 802.11p. In the beginning, all RSUs will repeat the first *Collection* phase to collect traffic information via CAMs of vehicles every time period p_v. Each CAM must contain the speed, location, heading, signature of the synopsis result S_c and public-key certificate P_c of the vehicle. In Fig. 4, it is assumed that the event E_1 occurs within the range of R_3 at time t_{1b}, and its corresponding rule is G_V (τ_v, m,$\mathbb{S}$,p_v) where τ_v is 10 times, S is equal to $\bar{V} < 5$km/hr and p_v is 10 sec, if the total number of rule matches m from the collected CAMs of different vehicles exceeds 10 times before p_v expired, the output of G_V is 1 and enters *Deduction* phase. The validation parameters (τ_r,$\mathbb{S}$,p_r) where τ_r is 20 times, S is equal to $\bar{V} < 5$km/hr and p_r is 30 sec will be generated at this phase, then broadcasted via DENMs at *Notification* phase and R_3 will also start the second *Collection* phase at the same time.

R_3 will enter *Judgment* phase and confirm the event if the total number of rule matches k from the collected CAMs of the new coming vehicles exceeds 20 times before p_r expired. After the event is confirmed, R_3 will enter *Transaction* phase and validate all event evidence, including signature verification. After this procedure, R_3 will announce the proven event to the nearby vehicles through DENMs at *Announcement* phase. Since no fresh *BH* is received after the previous $BH_{(t0,t1)}$, this first announcer will also create the new $BH_{(t2,t3)}$ and $BT_{(t2,t3)}$, then broadcast $BT_{(t2,t3)}$ via Ethernet to other RSUs in the same zone with the event evidence which belongs to the participated vehicles. As long as other RSUs receive this $BT_{(t2,t3)}$, the new validated event will be put into the MPT structure The PoE consensus procedure is illustrated with Fig. 5. After the event E_1 validated by R_3, the $BH_{(t2,t3)}$ is created and $BT_{(t2,t3)}$ with the evidence of E_1, called BT_{R3}, is broadcasted to other RSUs. After receiving BT_{R3}, each RSU will verify the event evidence of E_1 again to ensure the data integrity. If there is a second event E_2 that occurs within the scope of R_1, the corresponding BT_{R1} will be broadcasted to other RSUs after the event E_2 validated by R_1. After receiving BT_{R1}, each RSU will verify the event evidence of E_2 again. If this verification is successful, BT_{R1} will be combined with the previous BT_{R3} to form a union $BT_{R1 \cup åR3}$, reaching the consensus of the *local-chain*. Conversely, if the verification fails, the event cannot be added to the current $BT_{(t2,t3)}$. This PoE mechanism ensures that evidence of events is difficult to forge.

When the *local-chain* needs to be submitted to the *global-chain* for public access at t_{3a}, all RSUs will first commit the current MPT structure for synchronization. And the last block creator R_3 will be responsible for this submission process. Since the *local-chain* is maintained via Ethernet by each RSU in the same zone, each vehicle can get the latest events by requesting the latest block of the *local-chain* from any RSU.

In addition, when an accident occurs, the unproven event will be sent first to notify other nearby vehicles, then widely announced after the event has been validated. This two-pass event validation ensures that it is difficult for selfish or malicious vehicles to distribute fake events.

IV. EXPERIMENTS AND RESULTS

We use the NS-3 network simulator [38] to verify the design concept with the real traffic data from Traffic Information Service (TISV) in Taiwan [39]. One of the 3,617 vehicle detectors (VDs) of Taiwan Highway, VD-N1-N-34.900-M-LOOP, was chosen to demonstrate our framework and data from 2014/01/02 to 2014/01/14. This VD works as a RSU

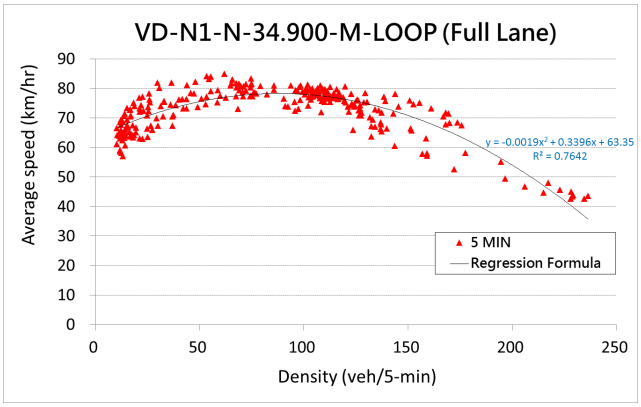


FIGURE 6. The impact of the density on the average speed of the 5min-VD.

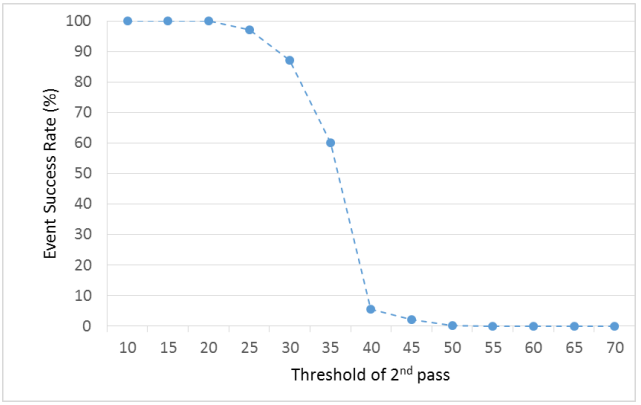


FIGURE 7. The impact of the threshold of the 2nd pass on the event success rate.

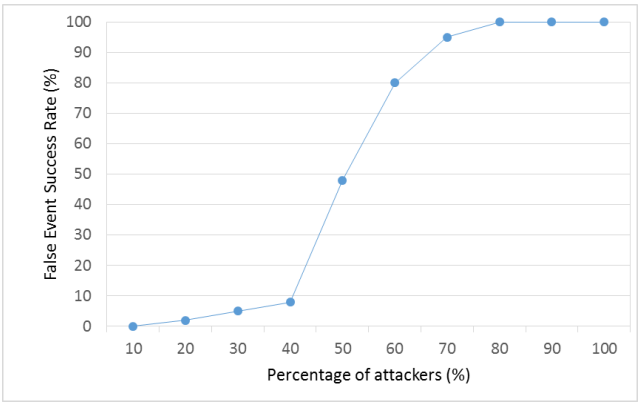


FIGURE 8. The impact of the percentage of attackers on the false event success rate.

TABLE 1. Parameters of simulation.

Descriptions	Values
For Event Validation	
MAC Type	802.11p
PHY Mode	6Mbps / 10MHz
the size of CAM	100 bytes
the size of DENM	150 bytes
velocity of vehicles	40-85 km/hr
vehicles	320 (5 min)
the fix CAM sending ratio	10 Hz (100 ms)
the fix DENM sending ratio	1 Hz (1 sec)
the expired time of 1st pass p_v	10 sec
the expired time of 2nd pass p_R	30 sec
the threshold of 1st pass τ_v	10
the threshold of 2nd pass τ_r	10 - 70
For Consensus Comparison	
the total RSU	16 - 160
the number of miners (PoW)	16
the number of authority nodes (PoA)	16
the number of generated blocks	6
average block generation interval	10 min
the number of events (transactions)	16
average size of block size	256 KB

with vehicles passing through it. The impact of density on average speed of the 5min-VD data is shown in Fig. 6. Based on the VD data, the average number of vehicles per day is 31,448 and the average speed is 72.5 km/hr. The parameters of simulation is listed in Table 1. Each simulation is running for twenty times to average. The size of a CAM is set to 100 bytes and contains the ECDSA signature and certificates. But the size of the actual captured packet is 164 bytes which contains the IEEE 802.11 Frame, Logical-Link Control and the UDP header. Similarly, the size of a DENM is set to 150 bytes but the actual captured is 214 bytes.

A. EXPERIMENT 1: NO INTERNAL ATTACKER

We implement the two-pass threshold-based event validation on the RSUs and use the VD data for simulation. In the Experiment 1, it is assumed no internal attacker is in the network. The impact of the threshold of the second pass τ_r on the event success rate is inspected and the result is shown in Fig. 7. When the threshold of second pass is set to 40, the success rate of event validation declines. That is because the density of the vehicle is not enough to meet the conditions. According to the result, the threshold of the second pass τ_r will be set to 15 to ensure a higher success rate.

B. EXPERIMENT 2: WITH INTERNAL ATTACKER

In Experiment 2, it is assumed internal attackers are in the network. The impact of percentage of attackers on the false event success rate is checked and the result is shown in Fig. 8. When the percentage of attackers is greater than 40%, the proposed framework will increasingly report the incorrect events. Therefore, no more than 40% of attackers can reduce the false positives rate in event reports below to 10%. This also indicates that an internal attackers can be detected in the proposed framework.

C. EXPERIMENT 3: COMPARISON OF CONSENSUS

In Experiment 3, PoW, PoA, and the proposed PoE consensus mechanisms were compared to RSUs ranging in numbers from 16 to 160. For PoW, the number of miners is set to 16. For PoA, the number of authority nodes is also set to 16. For the proposed PoE, the number of events in the same period is set to 16 as well. The block is generated every 10 minutes and the total of 6 blocks are generated for one hour. The simulation result of the impact of the number of RSUs on the synchronization time of different consensus algorithms is shown in Fig. 9. The result is not a perfect incremental curve which means the incremental relationship between synchronization time and the number of nodes is not very obvious. The result also shows that 16 events in a one-hour period take 22.4 sec to synchronize all 160 nodes, slightly better than PoW but worse than PoA. In addition, PoA has the less synchronization time because only public nodes need to verify the transactions and only exchange messages once. However, for PoW and PoE, each node needs to verify the transactions or the evidence of events, thus consuming more time.

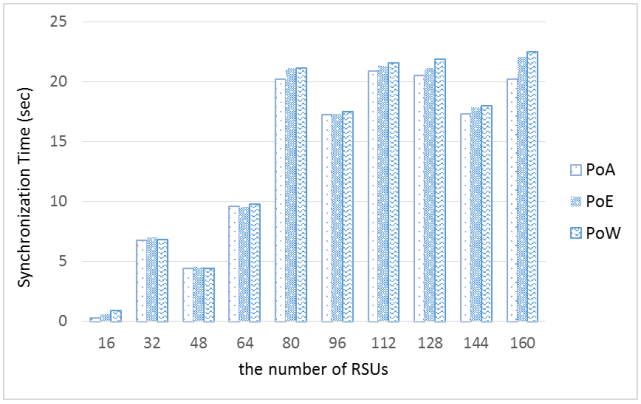


FIGURE 9. The impact of number of RSUs on the synchronization time of different consensus algorithms.

V. DISCUSSION

How to avoid the fraudulent transactions is the key technology of each consensus mechanism. We will discuss the proposed PoE mechanism with other approaches for vehicular network in this section. In Table 2, various common and the proposed consensus algorithms are compared. In the PoW approach, each node reaches a consensus by checking the hash value of the block and adjusts this hash value by changing a nonce to match the difficulty set by the target value when creating a block. The smaller the target value, the harder it is to find. Since each node can join to solve the hash puzzle, the network type can be public and decentralized. However, as the network expands, the difficulty of block generation is bound to increase and computing power will consume more.

PoS is similar to PoW, but the target value depends on the owned stakes of nodes. The more the owned stakes, the less difficult it is to set. Because part of the difficulty of PoS is lower than that of PoW, the efficiency is better than PoW. In the DPoS approach, the block producer is voted in by the node that owns the stake. Since the verification process is performed by a group of delegates, the network type is partially centralized. But because of this, the performance is better than PoS and can be expanded easily.

TABLE 2. Comparison of consensus mechanisms.

	PoW	PoS	DPoS	PoA	BFT	PoE
Mechanism	Solving the hash problem with the same difficulty	Solving the hash problem with the different difficulty	Negotiating between nodes	Trusting the public nodes	Negotiating between nodes	Event validation of nodes
The producer	The first hash finder	The stake owner	The stake owner	The trusted node	The trusted node	The RSUs according to the validation time
Network type	Public and totally decentralized	Public and decentralized	Partial centralized	Private or permissioned only	Private or permissioned	Permissioned
Efficiency	Slow and high energy consumption	Energy efficient	High energy efficiency and scalability	Fast and energy efficient	High scalability and throughput	Depends on the event occurrence

In PoA, only the known and verified identities can obtain the right to produce the block. So it is very fast and energy efficient. But because of the open nature of the producer, the network is always permissioned or private for security concern. In Byzantine Fault Tolerance (BFT), verifiers require three rounds of message exchange to tolerate BF nodes. Unlike PoA, verification only takes one round. Therefore, the performance of PoA is better than BFT. However, if we consider the above consensus mechanism to operate on VANETs, we will face some challenges and describe them as follows.

The blockchain is created by solving the hash problem in both PoW and PoS, that is, computing power is a big problem. Vehicles typically have limited electric power and it is difficult for the owner to provide such computing power. For the PoA approach, the trusted node is needed to be elected as the producer, i.e. the node will be revealed to the public. For vehicles, both mass transit, such as buses, cable cars, etc., and official vehicles, such as police cars, ambulances, blood donation cars, etc., can be the choice. Moreover, the vehicle is not always online and the maintenance of blockchain will exhaust the wireless network resource, especially the block producer needs to announce a new chain to all other nodes in VANETs. Therefore, it is recommended that central ITS stations or RSUs become miners and participants. The most existing literature is in the way [28], [32], [33].

On the other hand, for RSUs or infrastructure nodes, the existing approaches can solve the Byzantine problem if the power and energy is not a concern. However, extra computing power is needed for PoW and PoS. For other approaches, the trusted nodes are at risk if an internal attacker exists.

The proposed PoE is well-designed for VANETs. Unlike PoW or PoS, nodes are designed in PoE to take computing power for event validation rather than only solving the

difficult hash problems. In addition, the block producer can be verified through its event evidence by other nodes. It is difficult for an internal attacker to falsify an event description with correct evidence and it is also hard to adjust the timestamp for winning a producer. Recently, *Raft* is also a popular practical approach [15]. The producer is elected by randomized timers to support highly-available distributed systems; however, malicious nodes are also easy to make the system fail. Therefore, we believe that this PoE has great potential for VANET or other applications.

However, there is still an inefficiency. The PoE consensus algorithm is divided into two parts. The two-pass event validation exchanges traffic information through the wireless network. This part might have a transmission delay. Especially when the number of vehicles is too large, the solution is to reduce the exchange frequency. The other part is the two-phase transaction on blockchain running over the wired network, so there is no serious transmission delay, but when a vehicle requests a bulk of blockchain messages, it may cause congestion in the wireless network.

VI. CONCLUSION

The PKI-based framework in VANETs can provide fundamental security service, such as authentication, identity, non-repudiation and privacy. Attackers from the outside or Sybil intruders can be easily isolated. On the other hand, eavesdropping can also be avoided by using encryption algorithms [40]; however, it is still the problem against traitors or cheaters. Although a reputation system may be a solution but it hard to maintain the trustworthiness of all nodes.

The proposed BTEV framework mainly contains a two-pass threshold-based event validation mechanism and a two-phase consecutive transaction on the blockchain. The former can help identify the truth of events, i.e. messages from selfish or malicious nodes have no influence on the results. This is also verified by our simulation results. The latter can accelerate the submission of transactions to the blockchain. The *local-chain* is circulated only for RSUs in the same region. For this reason, vehicles can access the traffic information efficiently when coming a region. In addition, the election for the producer depends on the timestamp of event confirmation and each producer can be qualified by its own event evidence. Hence, it can save a lot of power consumption compared to PoW approach. It is worth mentioning that some researches such as *TrueBit* [41] use the verification game to solve the verifier's dilemma. We can consider adding this verification game for vehicles in participation to ensure the correctness and fairness of the entire blockchain.

In the proposed PoE strategy, the block producer can be verified by other nodes through the evidence of the traffic event description. However, in addition to event data from vehicles, there are various diversities of data types and forms, e.g., data from different mobile phones, different social media data like Facebook or Twitter, data from sensor networks, or D2D networks [42]. It is potential to extend PoE for other applications, such as an event validation for the weather, security, insurance claims, etc.

REFERENCES

[1] S. Kumar, L. Shi, N. Ahmed, S. Gil, D. Katabi, and D. Rus, "CarSpeak: A content-centric network for autonomous driving," in *Proc. ACM SIGCOMM*, Helsinki, Finland, 2012, pp. 259–270.
[2] U. Lee and M. Gerla, "A survey of urban vehicular sensing platforms," *Comput. Netw.*, vol. 54, no. 4, pp. 527–554, 2010. doi: 10.1016/j.comnet.2009.07.011.
[3] Y.-T. Yang and L.-D. Chou, "Position-based adaptive broadcast for inter-vehicle communications," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, May 2008, pp. 410–414.
[4] A. Hussein, F. García, J. M. Armingol, and C. Olaverri-Monreal, "P2V and V2P communication for Pedestrian warning on the basis of Autonomous Vehicles," in *Proc. 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Rio de Janeiro, Brazil, Nov. 2016, pp. 2034–2039.
[5] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, document ETSI EN 302 637-2 V1.4.0, 2018.
[6] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*, document ETSI EN 302 637-3 V1.2.1, 2014.
[7] J. Santa, F. Pereñíguez, A. Moragón, and A. F. Skarmeta, "Experimental evaluation of CAM and DENM messaging services in vehicular communications," *Transp. Res. C, Emerg. Technol.*, vol. 46, pp. 98–120, Sep. 2014.
[8] S. Gillani, F. Shahzad, A. Qayyum, and R. Mehmood, "A survey on security in vehicular ad hoc networks," in *Proc. Int. Workshop Commun. Technol. Vehicles*. Berlin, Germany: Springer, 2013, pp. 59–74.
[9] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Eng. J.*, vol. 54, no. 4, pp. 1115–1126, 2015.
[10] R. W. van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 779–811, 4th Quart., 2018. doi: 10.1109/COMST.2018.2873088.
[11] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. 27th IEEE INFOCOM*, Phoenix, AZ, USA, Apr. 2008, pp. 1238–1246.
[12] 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, 2009, Art. no. 125348. doi: 10.1155/2009/125348.
[13] F. G. Mármol and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 934–941, 2012. doi: 10.1016/j.jnca.2011.03.028.
[14] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic cash system," Tech. Rep., 2008.
[15] D. Ongaro and J. Ousterhout, "In search of an understandable consenus algorithm (extended version)," in *Proc. USENIX Conf. Annu. Tech. Conf. (USENIX ATC)*, 2014, pp. 305–320.
[16] A. Goranović, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, and T. Sauter, "Blockchain applications in microgrids an overview of current projects and concepts," in *Proc. IEEE 43rd Annu. Conf. Ind. Electron. Soc. (IECON)*, Oct./Nov. 2017, pp. 6153–6158.
[17] S. Burkhard and T. Bocek, "Smart contracts—Blockchains in the wings," in *Digital Marketplaces Unleashed*. pp. 169–184. [Online]. Available: https://link.springer.com/chapter/10.1007%2F978-3-662-49275-8_19. doi: 10.1007/978-3-662-49275-8_19.
[18] *Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)*, document ETSI TR 102 893 V1.2.1, 2017.
[19] E. B. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, no. 3, pp. 380–423, Jul. 2015.
[20] *Intelligent Transport Systems (ITS); Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats*, document ETSI TS 103 097 V1.3.1, Oct. 2017.
[21] A. Salem, A. Abdel-Hamid, and M. A. El-Nasr, "The case for dynamic key distribution for PKI-based VANETs," *Int. J. Comput. Netw. Commun.*, vol. 6, pp. 61–78. doi: 10.5121/ijcnc.2014.6105.
[22] *Intelligent Transport Systems (ITS); Security; Pre-Standardization Study on Pseudonym Change Management*, document ETSI TR 103 415 V1.1.1, 2018.
[23] H.-C. Hsiao, A. Studer, R. Dubey, E. Shi, and A. Perrig, "Efficient and secure threshold-based event validation for VANETs," in *Proc. ACM Conf. Wireless Netw. Secur. (WiSec)*, Hamburg, Germany, 2011, pp. 163–174.

[24] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1711–1720, Mar. 2016. doi: 10.1109/.TVT.2015.2405853.

[25] W. Gao, M. Wang, L. Zhu, and X. Zhang, "Threshold-based secure and privacy-preserving message verification in VANETs," in *Proc. 13th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Beijing, China, Sep. 2014, pp. 795–802.

[26] K. Wüst and A. Gervais, "Do you need a Blockchain?" in *Proc. IEEE Crypto Valley Conf. Blockchain Technol. (CVCBT)*, 2018, pp. 45–54.

[27] P. K. Sharma, S.-Y. Moon, and J.-H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart city," *J. Inf. Process. Syst.*, vol. 13, no. 1, pp. 184–195, 2017. doi: 10.3745/JIPS.03.0065.

[28] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, to be published. [Online]. Available: https://ieeexplore.ieee.org/document/8358773. doi: 10.1109/JIOT.2018.2836144.

[29] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, 2002.

[30] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. 19th IEEE Intell. Transp. Syst. (ITSC)*, Nov. 2016, pp. 2663–2668.

[31] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018. doi: 10.1109/ACCESS.2018.2864189.

[32] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Aug. 2018, pp. 674–679.

[33] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao. (2018). "Towards secure blockchain-enabled Interne0t of vehicles: Optimizing consensus management using reputation and contract theory." [Online]. Available: https://arxiv.org/abs/1809.08387

[34] *Intelligent Transport Systems (ITS); Users and Applications Requirements; Part 2: Applications and Facilities Layer Common Data Dictionary*, document ETSI TS 102 894-2 V1.3.1, Aug. 2018.

[35] T. Umedu, K. Isu, T. Higashino, and C. K. Toh, "An intervehicular-communication protocol for distributed detection of dangerous vehicles," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 627–637, Feb. 2010.

[36] (2018). *Main Specification: Merkle Patricia Trie*. [Online]. Available: https://github.com/ethereum/wiki/wiki/Patricia-Tree

[37] J. Poon and T. Dryja. (2016). *The Bitcoin Lightning Network: Scalable Off-chain Instant Payments*. [Online]. Available: https://lightning.network/lightning-network-paper.pdf

[38] *ns-3 Network Simulator*. Accessed: Oct. 16, 2018. [Online]. Available: https://www.nsnam.org/

[39] *Traffic Data Collection System (TDCS)*. Accessed: Oct. 16, 2018. [Online]. Available: http://tisvcloud.freeway.gov.tw/history/vd/

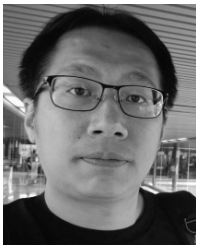
[40] *Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management*, document ETSI TS 102 940 V1.3.1, Apr. 2018.

[41] J. Teutsch and C. Reitwießner. (2018). *A Scalable Verification Solution for Blockchains*. [Online]. Available: https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf

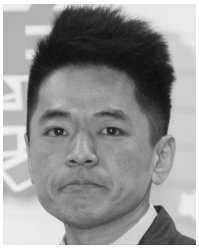
[42] F.-H. Tseng, J.-H. Hsueh, C.-W. Tseng, Y.-T. Yang, H.-C. Chao, and L.-D. Chou, "Congestion prediction with big data for real-time highway traffic," *IEEE Access*, vol. 6, pp. 57311–57323, 2018. doi: 10.1109/ACCESS.2018.2873569.

YAO-TSUNG YANG (S'10) received the M.S. degree in computer science and information engineering from National Central University, Taoyuan, Taiwan, in 2008, where he is currently pursuing the Ph.D. degree with the Department of Computer Science and Information Engineering. His research interests include software-defined networking, network function virtualization, vehicle ad hoc networks, artificial intelligence, and blockchain.

LI-DER CHOU (M'95) received the M.S. and Ph.D. degrees in electronic engineering from the National Taiwan University of Science and Technology, Taiwan, in 1991 and 1995, respectively. He was the Director of the Computer Center of National Central University and the Director of the Board of Taiwan Network Information Center. He was also the Deputy Director General of the National Center for High-Performance Computing, Taiwan, from 2013 to 2016. He is currently a Distinguished Professor with the Department of Computer Science and Information Engineering, National Central University, and the Secretary-General of National Central University, Taiwan. He holds five U.S. and 16 Taiwan invention patents. His research interests include SDN/NFV/SFC, vehicular networks, network management, broadband wireless networks, and the Internet services. He has published more than 200 papers in these areas. He was a recipient of the seven Best Paper Awards and the four Excellent Paper Awards from the international and domestic conferences. He was also a recipient of the two Gold Medal Awards and the four Silver Medal Awards in international invention shows held in Geneva, Moscow, London, and Taipei.



CHIA-WEI TSENG (S'17) received the M.S. degree in computer science and information engineering from National Dong Hwa University, Hualien, Taiwan, in 2006. He is currently pursuing the Ph.D. degree with the Department of Computer Science and Information Engineering, National Central University, Taiwan. His research interests include software-defined networking, vehicle ad hoc networks, and IPv6 protocol.



FAN-HSUN TSENG (S'12–M'18) received the Ph.D. degree in computer science and information engineering from National Central University, Taiwan, in 2016. He is currently an Assistant Professor with the Department of Technology Application and Human Resource Development, National Taiwan Normal University, Taipei, Taiwan. His research interests include mobile edge computing, 5G mobile networks, and artificial intelligence. He received the 2018 MOST Young Scholar Fellowship for his dedication to the research of engineering and technologies. He served as an Associate Editor-in-Chief for the *Journal of Computers* and an Associate Editor for *Human-centric Computing and Information Sciences*.

CHIEN-CHANG LIU received the M.S. degree in computer science and information engineering from National Central University, Taoyuan, Taiwan, in 1999, where he is currently pursuing the Ph.D. degree in computer science and information engineering. His research interests include software-defined networking, network function virtualization, and network management.