IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 26, 2019, accepted July 11, 2019, date of publication July 15, 2019, date of current version August 1, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2928753*

# Regional Blockchain for Vehicular Networks to Prevent 51% Attacks

**RAKESH SHRESTHA[1], (Member, IEEE), AND SEUNG YEOB NAM[2], (Senior Member, IEEE)**

[1]Yonsei Institute of Convergence Technology, Yonsei University, Incheon 21983, South Korea
[2]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea

Corresponding author: Seung Yeob Nam (synam@ynu.ac.kr)

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) supported by the Ministry of Education, Science and Technology under Grant 2013R1A1A2012006 and Grant 2015R1D1A1A01058595, in part by the Ministry of Science, ICT and Future Planning (MSIP), South Korea, through the Information Technology Research Center (ITRC) Support Program under Grant IITP-2019-2016-0-00313 supervised by the Institute for Information communications Technology Promotion (IITP), and in part by National Research Foundation of Korea through the Brain Korea 21 Plus Program (NRF) under 22A20130012814.

**ABSTRACT** The next generation of vehicles will be autonomous, connected, electric, and intelligent with distinct requirements such as high mobility, low latency, real-time applications, seamless connectivity, and security. Blockchain can provide a good solution to the issue of secure message dissemination or secure information sharing in vehicular networks with a weak trust relationship among the nodes. In this paper, we investigate the design of a regional blockchain for VANETs, where the blockchain is shared among nodes in a geographically bounded area. We investigate how to design the regional blockchain while achieving a low 51% attack success probability. We derive a condition that guarantees a low 51% attack success probability in terms of the numbers of good nodes and malicious nodes, the message delivery time, and the puzzle computation time. The condition can provide a useful guideline for selection of several control parameters guaranteeing the stable operation of the blockchain. We run several simulations to show the validity of the condition and investigate the effects of various parameters on the 51% attack success probability. Our analysis and simulation results show that maintaining a low message delivery time for good nodes is very important in protecting the stability of the blockchain system.

**INDEX TERMS** Blockchain, regional blockchain, security, 51% attack, immutability attack.

## I. INTRODUCTION

In recent decades, there has been a persistent increase in the number of smart and autonomous vehicles. Vehicular networks are used for traffic control, accident avoidance, parking management, and critical message dissemination [1]. According to a recent article [2], electric carmakers and tech giants from US, Europe, and China are developing driverless vehicles. The global market for smart and autonomous vehicles is growing rapidly and it is predicted that the market size will be expanded more than tenfold from 2019 to 2020. By the end of 2019, the autonomous vehicle market value is expected to reach $54.23 billion and it will increase to $556.67 billion by the end of 2026 [3]. Similarly, one electric vehicle maker, Tesla Inc. [4], is planning to provide "fully self-driving" vehicles to its customers by 2019. Autonomous vehicles, also known as driverless vehicles, use artificial intelligence software along with multiple sensors. The current semi-autonomous driving functions mainly focus on recognition and judgments, such as forward-collision and lane-change warnings based on sensors, such as light detection and ranging (LIDAR) and radar, attached to the vehicle. However, there is a limitation on the detectable range of the sensors attached to vehicles due to obstacles or weather conditions. Therefore, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications play an important role in message exchanges between vehicles. In a vehicular ad-hoc network (VANET), secure communication between the vehicles and the infrastructure is essential. If a hacker intrudes into normal vehicles or interferes vehicle communication via eavesdropping, jamming and spoofing attacks [5], then there might be serious accidents that may damage the vehicles or threaten the lives of the passengers. The main goal of the VANET is to disseminate critical-event information (such as accident reports) in a timely, secure, and accurate manner to ensure safe driving [6]. However, it is still a challenge

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

  

to disseminate critical-event information to the nodes in a targeted area under a dynamic vehicular environment and in the presence of untrustworthy information and dishonest vehicles [7], [8]. Most of the previous work on message security in VANETs uses centralized approaches. It is difficult to compute and manage all the information with a small delay to all the nodes under a central authority (CA) node. The main issue with the centralized mechanism is the single-point-of-failure problem. In order to overcome this issue, some research has focused on a distributed management scheme in a VANET [9]. However, there are other issues with the distributed management system such as distributed key management, content distribution, message trust and data privacy due to the dynamic nature of the VANET. This distributed trust mechanism might not work properly when there are very few, or a negligible number of neighboring vehicles, and the trust values may be inaccurate due to insufficient event information.

A security mechanism is required to ensure that malicious vehicles cannot manipulate, change, interfere with, or delete the critical-event messages in a VANET. If the safety messages generated by the vehicles can be recorded in a distributed database, then all the information will be transparent and be shared globally. This type of security can be achieved by using blockchain technology, which has recently gained attention and has great potential in diverse fields [10], [11]. Blockchain is an emerging decentralized and distributed computing platform that supports cryptocurrency applications such as Bitcoin, and it can provide security and privacy for those applications [12]. Blockchain can be used to maintain a history of traffic or accident events, which can work as a ground truth for the vehicles querying the information. The main motivation for using blockchain in a VANET is the strength of the blockchain, where all the nodes of the blockchain network store the blocks, and continuously validate the integrity of the blocks. Any changes to the blockchain are transparent and are publicly visible to all the network nodes, and the recorded information cannot be forged easily.

Recently, there has been a lot of interest in blockchain technology and many researchers study how blockchain can be used in geospatial systems such as energy micro grids and logistics [13], [14]. In this paper, we investigate the use of a regional blockchain in VANETs, which is a blockchain shared by the nodes within a physically bounded area. The regional blockchain is used in a geographically limited area, and thus, the end-to-end message delay can be reduced due to smaller hop counts and propagation delay.

We can consider two important requirements for the VANET blockchain. The first requirement is the timely dissemination of newly mined blocks, and the second one is the immutability of the information stored in the blockchain. If a malicious driver can easily modify traffic event information regarding some accident stored in the blockchain, then normal drivers may not trust the VANET blockchain. If a new block cannot be disseminated to the neighbor nodes in a short time, then the information contained in the new block may not contribute to the safe driving significantly. In this aspect, the conventional Bitcoin blockchain may not be the best solution for the VANET blockchain. In the Bitcoin blockchain, the blocks containing cryptocurrency transactions are globally shared. However, the traffic information in one country needs not be shared with other countries, if the border-crossing traffic is not allowed between those countries. Thus, the regional blockchain considered in this paper can be a good approach in reducing the block delivery time between the nodes belonging to a confined area. We believe that the regional blockchain can meet those main requirements faced by the blockchain for VANETs. Especially, we show that regional blockchains can be used for secure information sharing among the nodes with a low success probability of 51% attacks, if the blockchain is designed carefully.

In this paper, we investigate how to design a regional blockchain while maintaining a low 51% attack success probability. As discussed in [15], the blockchain systems can have many security issues. Among them, we concentrate on 51% attack in this paper. Many people believe that the information recorded in the blockchain after the consensus procedure cannot be modified, and this property is usually called immutability [16]. However, if a malicious group controls more than 50% of the total hash power of the machines in the blockchain network, that group can rewrite all the block history invalidating the information written in the previously accepted blocks. This attack is usually called 51% attack. Since this attack can undermine one important property of blockchain, i.e. immutability, this attack will also be referred to as *immutability attack* in this paper, and we focus on this problem. One reason to define a new terminology for this well-known attack is that we found that this attack is possible with a much smaller ratio of malicious nodes if they are connected with a relatively small delay, which will be discussed later in Sections V and VI.

In more detail, we derive a condition to guarantee a negligibly small immutability attack success probability. This condition can provide a guideline on selection of multiple control parameters ensuring the stability of the regional blockchain. The key contributions of our paper can be summarized as follows:

a) We derive a condition for a low success probability of immutability attack in terms of the numbers of good and malicious vehicles, the average puzzle computation time, and block message delivery delay.
b) Through simulation, we show that the immutability attack success probability can be maintained close to zero when the above condition is satisfied.
c) Our derived condition for this low immutability attack success probability can provide a useful guideline for the selection of several control parameters including message delivery delay between vehicles, puzzle computation time, number of vehicles etc., while guaranteeing stable operation of the regional blockchain.

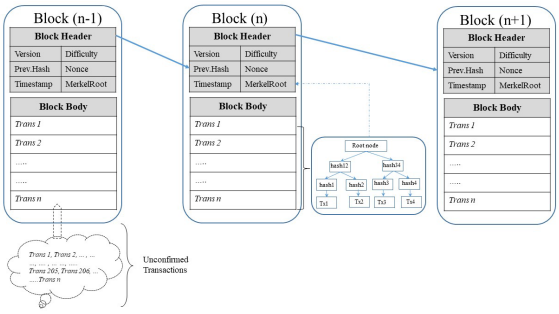


**FIGURE 1.** The working principle of blockchain.

Thus, the condition can be useful in designing new types of regional blockchains.

The remainder of our paper is organized as follows. Section II presents background and related work on blockchains. Section III discusses the regional blockchain and its usage in VANETs. Section IV deals with the attacker model targeting a regional blockchain. Section V derives the condition for a low success probability of the immutability attack, and provides a guideline for the selection of different control parameters. In Section VI, we describe the simulation environment and discuss the numerical results. Section VII investigates key issues related to message delay, with possible countermeasures for regional blockchains. Finally, Section VIII concludes the paper.

## II. RELATED WORK

This section provides a basic background of the blockchain and then presents related work regarding blockchain in VANETs and other fields. Blockchain is a distributed public ledger of digital events (or transactions) that are shared between network nodes [12]. Each event in a public database is verified by a majority of the nodes in the blockchain network. Blockchain has several advantages, such as decentralization, anonymity, chronological order of data, distributed security, transparency, and immutability [17]. Owing to the decentralized nature of the network, blockchain does not have a single-point-of-failure problem. There are basically two kinds of blockchain: public and private. A public blockchain is an open blockchain where anybody can participate in the network and interact with the blockchain without permission. The private blockchain is based on access control, and permission is needed to participate in the network. The regional blockchain can be in either of these two categories.

Each block in the blockchain contains the hash of its parent block recorded inside its header [12], [18], as shown in Fig. 1. Then, it is shared with other nodes in a distributed peer-to-peer network without any central authority. The consecutive hashes of blocks guarantee that transactions come in chronological order. Then, previous transactions cannot be modified without modifying their blocks and all subsequent blocks. A consensus mechanism, such as proof of work (PoW), is used to select the next block that will be added to the blockchain. PoW uses a mathematical puzzle that is very difficult to solve and easy to verify once the nonce value is known. It protects the blockchain from the 51% attack. As long as the computation power of honest nodes is greater than that of malicious nodes, the blockchain is considered secure [12], [19]. However, as we show in the remainder of this paper, the condition for secure operation of blockchain is more complicated than this.

In a VANET, message security is usually provided using voting-based approaches [20], [21]. Most approaches attempt to solve the issues related to secure message dissemination by using voting, or a similar method, that requests the opinions of neighboring vehicles to determine the trust level of the nodes.

However, the main issue with these types of approaches is that we cannot know if the feedback information obtained from neighbors, or the node itself is trustworthy or not. Some research was carried out using blockchain technology in a VANET. In [22], the authors used blockchain technology to support the distributed key management in heterogeneous VANETs. Similarly, in [23], the authors combined VANET and Ethereum's blockchain-based application concepts, enabling a transparent, self-managed, and decentralized system. The authors used smart contracts to run their application on the Ethereum blockchain. In [24], the authors presented a blockchain system that enables VANET nodes to transact services such as internet service, insurance service and transportation service, e.g. carpooling. The authors introduced a blockchain-based value transaction-layer protocol for the VANET to promote vehicle economy. Their work focused on the transaction protocol layer and provided an abstract architecture. They mentioned use cases for traffic congestion and token economy transactions for the VANET, but they did not discuss blockchain security issues.

There are research papers on utilizing a regional blockchain in energy micro grids. Micro grid technology focuses on a local energy grid that can work independently and autonomously from a central grid [25]. The micro grid uses local renewable resources efficiently, because the energy can be lost when it is transported over a long distance using power lines. The micro grid's efficiency can be improved by using local energy markets integrated with balancing mechanisms. In [13], the authors discussed local energy markets in a distributed concept based on consumers and prosumers that can deal with locally generated renewable energy directly within their region. The authors presented a private blockchain and simulated a local energy trading market between 100 housing units without the need of a central administrator. The authors only focused on local energy trading using blockchain, but they did not discuss security issues while implementing blockchain in a smart grid. Similarly, the authors in [26] presented a conceptual framework of a blockchain-based meter data-aggregation application in a regional electricity grid. A regional blockchain was presented based on a private blockchain that aggregates meter data in a certain geographic area. The nodes acting as smart meters are clustered together in a regional blockchain. Multiple regional blockchains are connected to the wide-area blockchain

maintained by the substation for storing data and processing the aggregated regional smart meter data. The authors in [27] introduced a new energy community model called PROSUME, which is an independent, autonomous, decentralized, and self-controlled monitoring system for exchanging energy from local sources. In PROSUME, the energy service utilizes local energy platforms based on permissioned blockchain [14]. It helps local community networks to share energy and optimize the cost and complexity to build micro grids. The authors used a smart contract, but did not consider security requirements while using blockchain in their system.

In a supply chain management system, the authors in [28] attempted to build a secure rice supply chain system based on blockchain to ensure safe distribution of rice from local retailers to wholesalers or supermarkets. The blockchain guarantees the traceability of the rice by storing all the events occurring within the rice supply chain as well as monitoring and recording the quality of rice in the blockchain to minimize fraud during the logistics process. However, the authors did not discuss any security issues for their blockchain. The authors in [29] proposed a new framework for access control that enables users to manage and control their data in the internet of things (IoT). The authors provided a reference model and implemented their model using Raspberry Pi with a camera module for monitoring children. Their model provides a decentralized access control mechanism based on proof of concept regional blockchain. They used new types of transactions to grant, delegate, get, and revoke access. The authors focused only on the access control mechanism for the IoT, but did not mention any blockchain security issues such as the 51% attack.

Although the blockchain technology is applied to diverse fields these days, the effect of key design parameters such as propagation delay on the security of blockchain system has not been investigated intensively yet. In [30], the authors investigated the effect of block propagation delay distribution on the blockchain fork probability. They mention that the increase of propagation delay may weaken the security of blockchain network. However, they did not provide any quantitative analysis on this matter, since they concentrated on explaining blockchain forks. In [31], the authors discuss optimal attacker strategies for double-spending attack and selfish mining under the given values of the parameters such as network propagation and block generation intervals. However, in this work, the network propagation parameter is not the propagation delay, but the connectivity of the adversary, i.e. the fraction of the network that receives the adversary's blocks in the case when the malicious and the honest miners release their blocks simultaneously in the network. The security of a given blockchain system against the double-spending attack is analyzed using the parameter $v_d$, the minimum transaction value that makes double-spending more profitable than honest mining. However, this parameter may not be appropriate in analyzing the security of blockchain systems against the 51% attack that attempts to forge a part of history on the blockchain, especially when the information recorded in the blockchain is not a monetary transaction, e.g. traffic event information in VANET. In this paper, we focus on the 51% attack which can undermine the immutability of blockchain systems, and investigate the security of blockchain systems by analyzing the success probability of 51% attack under the parameters such as the number of good nodes, the number of bad nodes, the message delivery time, and the puzzle computation time in detail.

## III. REGIONAL BLOCKCHAIN FOR VANETS

In this section, we introduce a regional blockchain for a VANET. The issues with global blockchains are propagation delay, scalability, and a long consensus convergence time that may not be suitable for real-time VANET applications. In most countries, the range of vehicles is geographically bounded, because vehicles may not be allowed to cross inter-country borders. Thus, the traffic event information of one country needs not be shared with the vehicles located in other countries. In this situation, applying a global blockchain for a VANET will be inefficient in terms of propagation delay, block size, puzzle computation time, etc. Therefore, we assume that each country will maintain a unique regional blockchain based on geographic borders. The advantage of the regional blockchain is that the block transmission delay between the vehicles can be reduced, and the message exchange rate between the vehicles can be decreased due to the limited number of vehicles in a given area.

In the regional blockchain, the event information that occurred in any specific location will be recorded in an unconfirmed event message pool of each node. Each vehicle in the regional blockchain acts as a miner or as a light node that simply generates event messages. Similar to the conventional blockchain, new blocks are built based on the event messages and the hashes of the previous blocks. The new blocks are chained together with the current block in a consecutive order to make a regional blockchain. The miners including vehicles and RSUs mine new blocks by using a consensus algorithm such as PoW [12]. Thus far, many consensus algorithms have been proposed including PoW, proof-of-stake (PoS), proof-of-capacity (PoC), practical byzantine fault tolerance (PBFT) [32], [33]. The regional blockchain can be built based on them. However, PoW used in Bitcoin and Ethereum is still a major consensus mechanism [34], and thus, we focus on PoW as a consensus mechanism in this paper.

After PoW puzzle computation, the new blocks are broadcast in the regional blockchain network. All the vehicles in the regional blockchain network will receive the new blocks, and they will verify the received blocks and update their blockchain. Thus, the regional blockchain stores all the history of event information that occurred in the given area.

If the history of all events in the given area is stored in a regional blockchain along with information about the nodes that reported the specific events, then the trust level of each node could be determined based on the reports stored in the blockchain. For example, let us assume all the event

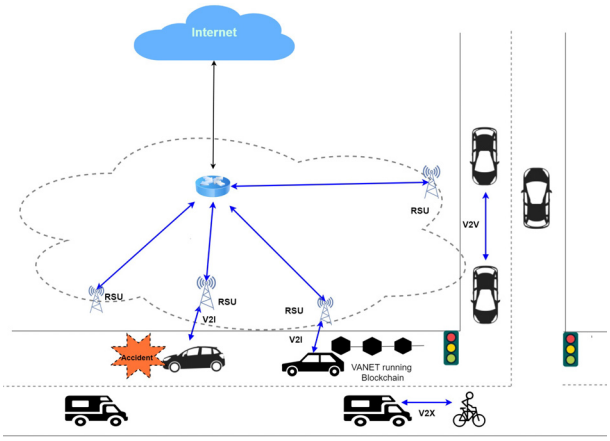


**FIGURE 2.** Secure message dissemination in VANET based on regional blockchain.

messages from each vehicle is recorded in the blockchain. If the information left in the blockchain is immutable, then the number of true messages and the number of false messages can be counted for each vehicle, and the trust level of a specific vehicle might be determined as the ratio of the true messages to the total messages from that vehicle [25]. However, our main focus is on the design of a regional blockchain, but not on the trust level evaluation for each vehicle. Thus, we want to investigate the issue of trust level evaluation separately in our future work. The assumptions needed to run a regional blockchain in VANETs are discussed below.

### A. ASSUMPTIONS

We assume that the vehicles participating in the regional blockchain are equipped with various sensors including on board units (OBUs), tracking sensors, and GPS. In the regional blockchain, each vehicle uses V2V, V2I, and vehicle-to-everything (V2X) communications [35], as shown in Fig. 2. We assume that the critical-event messages are disseminated within a region of interest (RoI) in a specific geographic area. In addition, we assume that video surveillance systems installed inside the vehicles, such as black boxes, act as a ground truth source for the critical-event information. The distributed video surveillance systems provide video frames to the road side units (RSUs) or edge devices that extract useful features, and information in real time using machine learning techniques [36]. Reinforcement learning used on the video frames over time can track and detect event information in real time, and the detection results can be used as forensic evidence for event information [16], [37]. We assume that the good vehicles follow the PoW-based blockchain protocol in the network, i.e., if a good vehicle receives an invalid block, then it will reject that block. We assume that good vehicles will get some kind of incentive that will motivate them to mine new blocks [35]. In this paper, we focus on how to reduce the success probability of the immutability attack by carefully selecting various control parameters for secure operation of the regional blockchain in a VANET.

**TABLE 1.** Event message format.

| Message body | |
|---|---|
| PID | Pseudo ID of the node |
| Pub address: | Public key |
| Event ID | ID of event |
| Event Type | Types of event |
| TimeStamp | Event timestamp |
| Location | Event location |
| Direction | Driving Direction |

### B. EXAMPLE OF A REGIONAL BLOCKCHAIN FOR VANETS

We consider a regional blockchain for VANETs because the conventional global-scale blockchain might be unsuitable. The regional blockchain for the VANET stores event information instead of transactions. Similar to the Bitcoin blockchain, the regional blockchains store and manage event information in a distributed manner.

When a vehicle encounters events on the road such as traffic jams, accidents, slippery road, etc., it will broadcast an event message with several parameters. All the vehicles broadcast their positions through beacon messages indicating the vehicles' location at a particular time. Before broadcasting the messages, each vehicle generating an event message verifies the event information. The event message contains information such as pseudo ID, event type, event ID, location, direction, and timestamp, as shown in Table 1. Such event messages are stored in the unconfirmed event message pool of each vehicle. The vehicles collect different event messages from the unconfirmed message pool. They check each event message based on evidence with regard to the sender vehicle's event location, event ID, driving direction, speed, timestamp, and the contents of a surveillance video. If there is no problem in the selected traffic event message, the vehicle generates a new block by solving a PoW puzzle. The vehicle then broadcasts the new block to the regional blockchain network. When other vehicles receive a newly created block, they verify that the block's hash is valid. After block verification, the vehicles continue constructing a new block using the hash of the last accepted block.

The verifiers can use the following message verification policies to know the trustworthiness of a given message.

- Check if the message is first-hand information
- Check the timestamp
- Check location, direction, and speed of the vehicle
- Collect supporting information regarding the particular event, such as messages received from neighboring vehicles located near the event location, video surveillance data, etc.

When new miner vehicles join the blockchain, they synchronize their copies of the blockchain against those of other vehicles in the network. All vehicles have their own copies of the regional blockchain in a distributed network. Independent validation of each new block by each vehicle in the network ensures that malicious vehicles cannot easily forge a history of the traffic events. In addition, each block depends on the

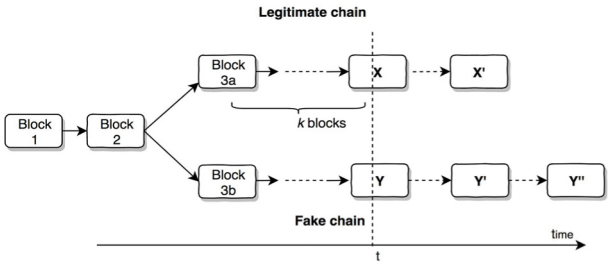


**FIGURE 3.** An example of immutability attack.

previous block's hash, and therefore, altering or forging a block is very challenging, and needs significant computation power to change the successor blocks. If consensus on the current state is accomplished by all the participating miner vehicles in the regional blockchain network, then this blockchain will be used as a ground truth source for the next block. Even if any malicious vehicle or group tries to modify the block contents, they would have to redo this complex work. Adopting the regional blockchain in vehicular networks is not straightforward because of the security issues, such as the immutability attack.

## IV. ATTACKER MODEL

In a VANET, the 51% attack or the immutability attack occurs, when the attacker nodes attempt to modify the contents of an old block in the blockchain. The attacker nodes might collaborate with each other to create an attacker pool and take control of the regional blockchain network. The nodes in the attacker pool might have a relatively short message delay between them. We assume that the message delivery time between malicious nodes is shorter than or equal to the message delivery time between good nodes. The short message delay between the nodes within the attacker pool can contribute to the fast growth of the blockchain on the attacker's side, which will be discussed in more detail later. When the malicious group's chain length exceeds that of the good group, the good group will accept the longer chain, leading to the success of the immutability attack by the malicious group, as shown in Fig. 3.

We assume that multiple malicious nodes form a group to launch an immutability attack on a commonly selected block, e.g. block 3a in Fig. 3, and they grow their own chain by rejecting the blocks from the good nodes until their immutability attack succeeds. We want to introduce one important parameter, $k$, which affects the success probability of the immutability attack by the malicious group. In Fig. 3, $X$ denotes the last legitimate block in the regional blockchain at time $t$, and this block is called the head-of-line (HoL) block at time $t$. In this figure, the colluding attackers want to change the contents of block 3a. The distance between the HoL block and this old block is $k$, which will be referred to as the initial chain depth (ICD) throughout this paper. We can easily expect that the immutability attack will be less successful as the value of $k$ increases. The immutability attack succeeds only when the chain length of the malicious group gets longer than that of the good group. Thus, for a sufficiently large value of $k$, the immutability attack success probability can be reduced close to zero if some condition is satisfied, and we will investigate this condition in more detail hereafter.

**TABLE 2.** Abbreviation of notations.

| *Notations* | *Descriptions* |
|---|---|
| $m$ | Number of good vehicles |
| $n$ | Number of malicious vehicles |
| $1/\lambda$ | Puzzle computation time of a single vehicle |
| $P_g$ | Block delivery time between any pair of good vehicles |
| $P_m$ | Block delivery time between any pair of malicious vehicles |
| $X(t)$ | Length of the chain grown by good vehicles at time t |
| $Y(t)$ | Length of the chain grown by malicious vehicles at time t |
| $k$ | ICD, i.e., difference between $X(t)$ and $Y(t)$ just before attack |
| $S_1$ | Random variable denoting the first block-generation time |
| $q$ | Random variable denoting puzzle computation time |
| $\mu$ | Service rate of queueing system |
| $\rho$ | Offered load of queueing system |
| $l$ | Queue length |

## V. CONDITIONS FOR A LOW SUCCESS PROBABILITY OF IMMUTABILITY ATTACK

In this section, we derive the condition required to lower the success probability of the immutability attack in terms of the following parameters: number of good vehicles ($m$), number of malicious vehicles ($n$), average puzzle-computation time of a single node ($1/\lambda$), and node-to-node block delivery delay ($P$). Before detailed derivation of the relation, we revisit the assumptions required for the analysis. The notations used in the derivation of the relation are summarized in Table 2.

We assume that each of the good and malicious vehicles has the same processing power to simplify the analysis. However, the computation power of the malicious group can be adjusted by changing the number of malicious vehicles ($n$). $q$ denotes a random variable corresponding to the puzzle computation time of a single vehicle. Then, we can assume that $q$ has an exponential distribution with parameter $\lambda$, i.e. $q \sim Exp(\lambda)$ [38], [39]. All the mining vehicles are classified into two groups: the good vehicle group and the malicious vehicle group (i.e. attacker pool). Each vehicle in the good vehicle group behaves in a normal manner as a usual mining vehicle without any collusion with other vehicles. When a good vehicle receives a new block, if the length of the chain corresponding to the new block is longer than that of the current chain that the vehicle is utilizing to generate a new block, it will accept the new chain by quitting its current puzzle computation. This will be referred to as *the longest chain rule* in this paper. However, we assume a different behavior for the malicious vehicles. Each malicious vehicle

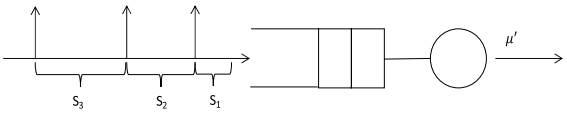


**FIGURE 4.** GI/G/1 queue for modeling *Q(t)*.

colludes with other malicious vehicles to successfully launch the immutability attack. Each malicious vehicle knows the members of the malicious group, and receives the newly generated blocks only from members of this group while ignoring blocks from the normal group.

In order to consider the worst-case scenario, we assume that the malicious vehicles are located geographically close to each other, and the message delivery time among them is shorter than for the good vehicles. In other words, the malicious group members can exchange the newly generated blocks with other vehicles in the same group with a smaller delay of $P_m$. On the other hand, we assume that the message delivery time is fixed to a constant $P_g$ for any pair of good vehicles, in order to simplify the problem. The message delivery time between the good group and the malicious group is assumed to be $P_g$ as well.

We now investigate the meaning of success for the immutability attack, and how it can be defined mathematically. Let us consider a case where the malicious group attempts to change the contents of an old block in the current blockchain, which is $k$ blocks ahead of the HoL block in the chain. The immutability attack is successful when the length of the chain grown by the malicious group exceeds that of the chain grown by the good group at any moment over time because of the longest chain rule of the normal vehicles. $X(t)$ and $Y(t)$ denote the length of the chain grown by the good group and that of the chain grown by the malicious group at time $t$, respectively. Then, the immutability attack fails when $\min_{t\geq 0} X(t) - Y(t) \geq 0$, and thus, we have

$$\Pr(\textit{double spending attack fail}) = \Pr(\min_{t\geq 0}\{X(t) - Y(t)\} \geq 0 | X(0) - Y(0) = k). \quad (1)$$

If we put $Q(t) = X(t) - Y(t)$ under the condition $Q(0) > 0$, then $Q(t)$ can be considered as the queue length of the below queueing system until $Q(t)$ becomes zero. We assume that the length of the blockchain of the good group is longer than that of the blockchain of the malicious group by $k$ blocks at time 0, and all the good and malicious vehicles simultaneously start puzzle computation on a new block at $t = 0$. We also assume that every vehicle can access the same list of messages, and there are a sufficiently large number of messages to mine without any discontinuity.

In Fig. 4, $S_1$ is a random variable denoting the first block-generation time from the good group since $t = 0$, and this will be determined by the vehicle that solves the puzzle earliest from among the $m$ good vehicles. The vehicle that generated the first block in the good group has the advantage of working on the puzzle for the next block earlier than other vehicles by message delivery time $P_g$. If this vehicle does not complete the second puzzle computation within $P_g$ from the first puzzle-computation time, $S_1$, then it needs to fairly compete with other vehicles in the good group. Let $S_i$ $(i = 2, 3, 4\ldots)$ denote the time interval from the $(i$-1)-th block-generation epoch to the $i$-th block-generation epoch. Then, $Q(t)$ increases by 1 at the interval of $S_i$, and thus, the block generation from the good group forms the arrival process in Fig. 4. Whenever the malicious vehicles find a new block, $Q(t)$ decreases by 1 from the definition of $Q(t)$, and thus, the block generation from the malicious group forms the departure process in Fig. 4. If we assume zero propagation delay among the malicious vehicles, the service rate of the queue $(\mu')$ becomes $n\lambda$, when the puzzle solution-generation rate of a single vehicle is $\lambda$.

From the definition of $S_1$ and $S_i$ $(i = 2, 3, 4\ldots)$, we can easily find that

$$S_1 \sim Exp(m\lambda).$$
$$S_i\,(i \geq 2) = \begin{cases} q|_{q\leq P_g}, & \text{if } q \leq P_g, \\ P_g + S_1, & \text{if } q > P_g, \end{cases} \quad (2)$$

where $q$ is a random variable denoting the puzzle computation time of a single vehicle as mentioned above, and $q|_{q\leq P_g}$ means a random variable with a truncated exponential distribution having zero density over $P_g$. Then, the arrival rate of the queueing system $(\lambda')$ can be expressed as $1/E[S_i]$ $(i \geq 2)$, and the queueing system becomes a GI/G/1 queue. When the offered load $\rho = \lambda'/\mu'$ is larger than 1, the queueing system becomes unstable, and $\lim_{t\to\infty} Q(t) = \infty$ [40]. If $Q(t) = X(t) - Y(t)$ diverges to infinity, then for an arbitrary positive queue length $l$, it is possible to find $t'$ such that

$$Q(t) > l, \quad \forall t > t'.$$

Thus, $Q(t)$ is positive for $t > t'$. Let us investigate $Q(t)$ for $0'$. The puzzle computation time of each vehicle has a lower bound of a fixed number of CPU clock cycles, which corresponds to the puzzle resolution in its first attempt. This is the minimum interval where either $X(t)$ or $Y(t)$ retains the same value before their values increase by 1, and $X(t)$ or $Y(t)$ change only by 1 whenever they change. Since the interval $[0, t]$ is finite, $Q(t)$ cannot diverge to minus infinity during this finite interval, even though the malicious vehicles resolve the puzzles much faster than the normal vehicles.

If we put $Q_{min} = \min_{0\leq t\leq t'} Q(t)$,
then, $Q(t) \geq l' = \min\{0, Q_{\min}\}$ for $t \geq 0$, since $l > 0$.
If we put $Y'(t) = Y(t) - |l'|$,
then we have,

$$Q'(t) = X(t) - Y'(t) = X(t) - Y(t) + |l'| = Q(t) + |l'| \geq 0, \quad \text{for } t \geq 0.$$

This means that if we increase the value of $k$ sufficiently by having the malicious group work on an older block, then the failure probability of the immutability attack can be maintained close to 1 according to (1). We now investigate the condition for the unstable queueing system, i.e. $\rho = \lambda'/\mu' > 1$, in more detail.

The expectation of $S_i$ given in (2) can be obtained as

$$\begin{aligned} \mathrm{E}[S_i] &= \Pr\left(q \le P_g\right) E\left[S_i | q \le P_g\right] \\ &\quad + \Pr\left(q > P_g\right) E\left[S_i | q > P_g\right] \\ &= \frac{1}{\lambda} - \left(\frac{1}{\lambda} - \frac{1}{m\lambda}\right) e^{-\lambda P_g} \end{aligned} \tag{3}$$

Let $T_i$ $(i = 2, 3, 4 \ldots)$ denote the time interval from the $(i\text{-}1)$-th block-generation epoch to the $i$-th block- generation epoch among the malicious vehicles. Then, $\mu'$ can be expressed as $\mu' = 1/E[T_i]$. By following the derivation of $\mathrm{E}[S_i]$ in (3), $E[T_i]$ can be obtained as follows:

$$E[T_i] = \frac{1}{\lambda} - \left(\frac{1}{\lambda} - \frac{1}{n\lambda}\right) e^{-\lambda P_m}. \tag{4}$$

where $P_m$ is the message delivery time between two vehicles in the malicious group, and we also assume that this value is the same for each pair of vehicles in the malicious group, in order to simplify the analysis. We have $\rho = \lambda'/\mu' = E[T_i]/E[S_i]$. By combining (3) and (4), it is possible to express the instability condition $\rho > 1$ in terms of $n$, $m$, $E[q]\,(= 1/\lambda)$, $P_g$, and $P_m$ as follows:

$$1 - \frac{1}{n} < \left(1 - \frac{1}{m}\right) e^{-\frac{P_g - P_m}{E[q]}}. \tag{5}$$

Thus, we can say that for a sufficiently large $k$, if the condition of (5) is satisfied, the immutability attack success probability can be maintained close to zero. Let us consider a simple example where $P_g = P_m$, i.e. the malicious group and the normal group have the same propagation delay. In this case, (5) is simplified to

$$m > n.$$

This means that for a sufficiently large $k$, the immutability attack can be prevented with a probability close to 1 as long as the good vehicles outnumber the malicious vehicles under the assumption that the CPU performance of every vehicle is the same, which is consistent with the common belief of the 51% attack. If we solve (5) in terms of $E[q]$, then we obtain

$$E[q] > \frac{P_g - P_m}{log\left(\frac{1-\frac{1}{m}}{1-\frac{1}{n}}\right)}. \tag{6}$$

This inequality provides a lower bound of the average puzzle-computation time,$E[q]$, which can prevent the immutability attack with a very high probability for a sufficiently large $k$, when the values of $m$, $n$, $P_g$, and $P_m$ are given. As an example, when $m = n$, the lower bound on the right-hand side of (6) diverges to infinity, and this means that the immutability attack cannot be prevented with a finite value of $E[q]$. However, if $m > n$, then the lower bound on the right-hand side has a finite value, and (6) can provide a useful guideline on the average puzzle-computation time. We also find that $E[q]$ should be proportional to the gap between $P_g$ and $P_m$. In other words, the message delays of the good group and the malicious group also significantly affect the stability of the blockchain system.

**TABLE 3. Simulation environment for simulator validation.**

| Parameters | Values |
|---|---|
| # of nodes in the blockchain network | 6000 |
| Average block generation interval in the network | 10 minutes |
| Average block delivery time | 8.7 seconds |

**TABLE 4. Stale block rates measured by two simulators (a) unsolicited block push mechanism used for block propagation and (b) standard block propagation mechanism.**

| | Our simulator | NS3 Bitcoin simulator [31] |
|---|---|---|
| Stale block rate | 1.43% | (a) 0.13% - (b) 1.88% |

## VI. NUMERICAL RESULTS

### A. SIMULATION SETUP

In order to evaluate the validity of the stability condition derived in Section V, we developed a discrete-event blockchain simulator using C++. We performed simulations to analyze the success probability of an immutability attack for diverse sets of blockchain control parameters. The control parameters include the numbers of good and malicious vehicles, average puzzle-computation time, and block delivery time. We also investigated the effect of the difference between the good-vehicle chain length and the malicious-vehicle chain length, i.e. ICD ($k$).

The simulations were performed on desktop computers running Windows 10, with a 3.20 GHz processor and 8 GB of main memory. All the simulations were run considering the stability condition given in (5). We assumed that each of the good and malicious vehicles has the same computational capacity.

### B. SIMULATION RESULTS

In [31], the authors made a Bitcoin blockchain simulator using ns-3, a popular discrete-event simulator, to compare different types of blockchain applications, including Bitcoin and Litecoin. They verified the validity of their simulator by comparing the stale block rate measured in the real Bitcoin network with that obtained from their simulator. The stale block means the block that is not included in the main chain of the longest length, when a fork is resolved [31], and the stale block rate is defined as the ratio of the number of stale blocks to the total number of blocks added to the final blockchain during the measurement period. Thus, we validate our simulator by comparing the stale block rate obtained by our tool with that obtained by the simulator of [31].

Table 3 shows the parameters considered for this simulation. The detailed values are determined based on the simulation environment considered in [31]. Table 4 compares the stale block rates measured by two different simulators over 10000 blocks. In our simulator, the block delivery time is a control parameter, and if the value is selected by a user, that value is applied to each pair of blockchain nodes. Thus, our simulator assumes the maximum connectivity [30], which corresponds to the full mesh connection among the

**TABLE 5. Summary of simulation scenarios.**

| Scenario no. | No. of good vehicles (m) | No. of malicious vehicles (n) | Average calculation time (sec) | Message delivery time (Good group) ($P_g$) | Message delivery time (Malicious group) ($P_m$) | ICD (k) |
|---|---|---|---|---|---|---|
| 1 | 12, 14, 15 | 10 | 100 | 1 | 0 | 5~100 |
| 2 (a, b) | 200, 250, 300, 400 | 100 | 100 | 0.5 | 0 | 5~100, 10~1000 |
| 3 | 2000, 2500, 3000 | 1000 | 100 | 1 | 0.95 | 1~150 |
| 4 | 200 | 100 | 100 | 1 | 0.1 ~ 1 | 10 |
| 5 | 200 | 100 | 10 ~ 1000 | 1 | 0.95 | 10 |
| 6 | 100~3000 | 400 | 100 | 1 | 0.8, 0.9 | 100 |
| 7 | 400 | 100~1500 | 100 | 0.9 | 1 | 100 |

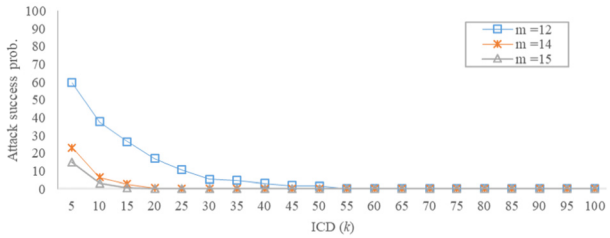


**FIGURE 5. Immutability attack success probability vs. ICD ($k$) for $n = 10$ (scenario 1).**

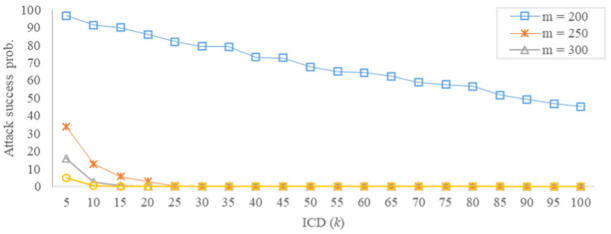


**FIGURE 6. Immutability attack success probability vs. ICD ($k$) for $n = 100$ (scenario 2 (a)).**

blockchain nodes, to reflect the assumptions made for the analysis in Section V. Table 4 shows that the stale block rate measured by our simulator belongs to the range obtained from the simulator of [31], even in the presence of the simplifying assumption on the block delivery time. Since our simulator reflects the collusion attack scenario of Section V and it is optimized in terms of the simulation time, all the subsequent scenarios are tested based on our simulator.

We considered seven different scenarios by varying parameters such as the numbers of good and malicious vehicles, ICD ($k$), the message delivery time, and average puzzle-computation time. The simulation scenarios are summarized in Table 5. We investigated the stability of the regional blockchain in terms of the success probability of the immutability attack. We calculated the attack success probability by averaging the simulation results for 1000 simulation runs.

In the first scenario, the numbers of good and malicious vehicles are small. Fig. 5 shows the results of the first scenario. We calculated the immutability attack success probability by setting the number of malicious vehicles at 10 and varying the number of good vehicles. We set the average puzzle-computation time to 100 seconds, the message delivery time of good-vehicle group is one second, and that of malicious vehicle group is zero seconds. We assumed that the malicious vehicles collude with each other to form an attacker pool with zero message delay. When the number of good vehicles is 12, the immutability attack success probability is high for a small value of $k$. It decreases as the value of $k$ increases and it converges to zero after $k$ goes over 55.

When the number of good vehicles is 14, the immutability attack success probability decreases to 23% for $k = 5$ and becomes zero after $k = 30$. Similarly, when the number of good vehicles is 15, the immutability attack success probability decreases to 15% for $k = 5$ and becomes zero for $k = 20$. Thus, we find that the immutability attack success probability can be maintained close to zero for a sufficiently large value of $k$ as long as the stability condition of (5) is valid, which agrees well with the conclusion of the analysis in Section V.

In the second scenario, we set the number of malicious vehicles to 100 and changed the number of good vehicles from 200 to 400. The second scenario consists of two subscenarios. Scenario 2 (a) focuses on smaller values of $k$, whereas Scenario 2 (b) covers a wider range of $k$ to show the convergence of the immutability attack success probability for large values of $k$. Fig. 6 shows a rather high success probability for smaller values of $k$ when $m = 200$. As the number of good vehicles increases, the immutability attack success probability decreases drastically and converges to zero. When the number of good vehicles is 400 and $k = 5$, the success probability is around 5%, and it converges to zero after $k = 15$. However, when the number of good vehicles is 200, the immutability attack success probability reaches about 45% for $k = 100$. We ran additional simulations to see the trend for larger values of $k$, when the number of good vehicles is 200. Fig. 7 shows that for a sufficiently large $k$, the immutability attack success probability approaches zero.

In the third scenario, we increased the number of good and malicious vehicles from hundreds to thousands. Fig. 8 shows the result for this scenario. When the number of good vehicles is 2000, the immutability attack success probability is over 95% for small values of $k$. However, the success probability decreases as the value of $k$ increases. The success probability reaches zero for $k = 150$, as shown in Fig.8. When the

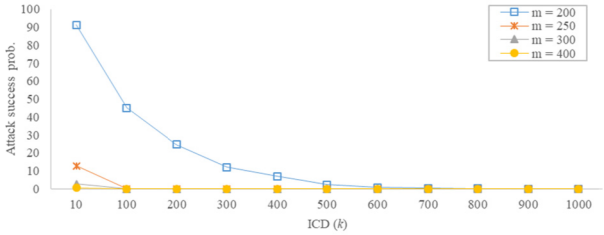


**FIGURE 7.** Immutability attack success probability vs. ICD ($k$) for $n = 100$ (scenario 2(b)).

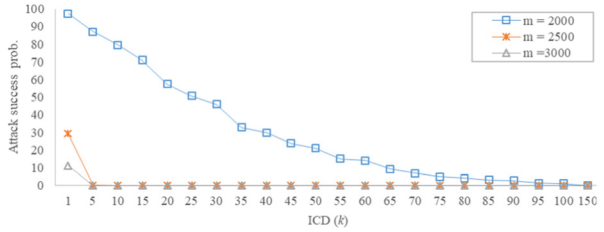


**FIGURE 8.** Immutability attack success probability vs. ICD ($k$) for $n = 1000$ (Scenario 3).

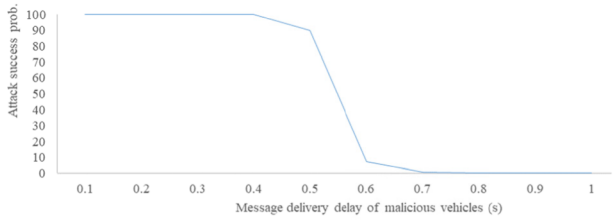


**FIGURE 9.** Immutability attack success probability vs. message delivery delay of malicious vehicles for $P_g = 1$ (scenario 4).

number of good vehicles is high (up to 2500 or 3000), the immutability attack success probability drastically decreases and converges to zero, even for small values of $k$. This shows that if the stability condition of (5) is satisfied, the immutability attack can be prevented effectively for a sufficiently large value of $k$.

In the fourth scenario, we calculated the immutability attack success probability against the different values for the message delivery delay of the malicious group. The message delivery time of the good group is fixed to one second. We set the value of $k$ to 10, and the numbers of good vehicles and malicious vehicles are fixed at 200 and 100, respectively. All other parameters for the fourth scenario are given in Table 5. The immutability attack success probability remains at 100% for the block propagation delays of less than 0.4 seconds, and it starts to decrease with a higher message delay for the malicious vehicles. The immutability attack success probability becomes zero when the message delay of the malicious vehicles is greater than or equal to 0.8 seconds in Fig. 9. Thus, we find that the message delivery delay of the malicious group significantly affects the success of the immutability attack. Especially, this simulation result implies that if the message delivery delay of the malicious group is very low, the 51% attack can be successful only with 33% (= 100/300) of the total computation power.

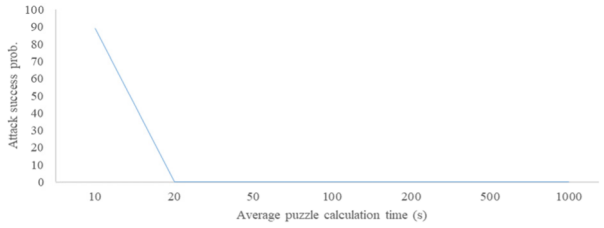


**FIGURE 10.** Immutability attack success prob. vs. average puzzle calculation time (s) for $P_g = 1$and $P_m = 0.95$ (Scenario 5).

In the fifth scenario, we calculated the immutability attack success probability against the different values of average puzzle-computation time. The detailed parameters for the simulation are given in Table 5. For a low average puzzle-computation time of 10 seconds, the attack success probability is around 90%. When the average puzzle-computation time becomes 20 seconds, there is a sharp reduction in the immutability attack success probability. The immutability attack success probability becomes zero at the average puzzle-computation time of greater than 20 seconds, as shown in Fig. 10. Thus, a higher puzzle computation time can be helpful in preventing the immutability attack, which agrees with the conclusion of (6) in Section V.

In the sixth scenario, we ran the simulation to investigate the effect of the gap in message delivery delay between the good group and the malicious group on the immutability attack success probability. The parameters for this scenario are given in Table 5. We ran simulations for a large number of malicious vehicles, i.e. 400, with different message delivery times for the malicious group. The message delivery time for the good group is fixed to one second. When the message delivery time of the malicious group is 0.8 seconds, the message delay gap between the good and malicious groups becomes 0.2. The immutability attack success probability is 100% even for a large number of good vehicles (e.g. 1800). If we increase the number of good vehicles further, then the immutability attack success probability decreases and reaches zero. When the message delivery time of malicious group is increased from 0.8 seconds to 0.9 seconds, then the message delay gap between the good and malicious groups becomes 0.1. In this case, the immutability attack success probability drops to zero for a relatively smaller number of good vehicles (i.e. 700). This graph shows that even a small difference in the message delivery delays between the good group and the bad group can affect the immutability attack success probability significantly. We find that as the message delay gap between the good group and the bad group increases, the bad group can launch the immutability attack successfully with a smaller number of bad group members compared to the number of good group members. In other words, it shows that 51% attack is possible with a small ratio (<0.5) of malicious nodes if the message delay for the malicious group is sufficiently short.

The last scenario is very similar to the previous scenario. In this scenario, the message delay for the good group (0.9 seconds) is shorter than that for the malicious

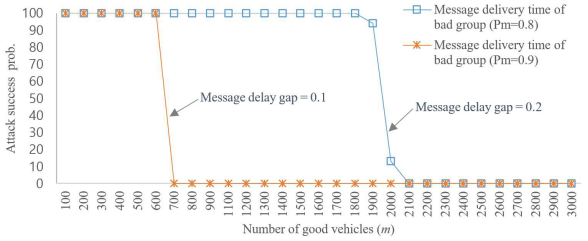


**FIGURE 11.** Immutability attack success probability vs. number of good vehicles ($m$) for $P_g = 1$ (scenario 6).

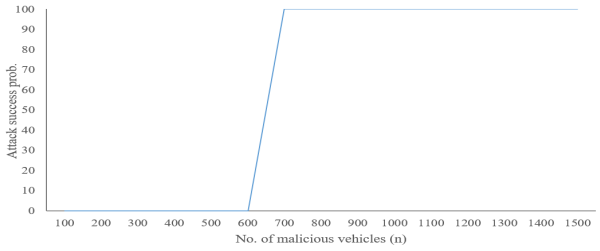


**FIGURE 12.** Immutability attack success probability vs. number of malicious vehicles ($n$) for $P_g = 0.9, P_m = 1$(scenario 7).

group (1 second). Since the message delay has been reversed between those two groups, we fixed the number of good nodes ($m$) to 400, and changed the number of malicious nodes ($n$) from 100 to 1500. Fig. 12 shows that 51% attack cannot succeed even when $n$ is 600 for $m = 400$. Thus, we find that the blockchain system can be protected from the 51% attack effectively even with a smaller number of good nodes when $P_g < P_m$.

## VII. MESSAGE DELAY RELATED ISSUES AND COUNTERMEASURES

The regional blockchain may not be stable if the message delivery delay of the malicious group is significantly shorter than that of the good group. In a VANET, the malicious vehicles might create a pool of attackers to reduce the message delivery delay between them. On the other hand, the message delivery delay among the good group members might be longer than that. In this case, stable operation may not be guaranteed, even though we increase the number of good vehicles significantly. If the gap between the message delivery delays of the good vehicle group and the malicious vehicle group is reduced, then the immutability attack can be prevented, as shown by the simulation results in Section VI. The issue of speeding up the propagation of blocks in the Bitcoin network has been discussed in [30], [31]. The authors of [30], [31] recommended minimization of verification, pipelining of block propagation, increase of connectivity, unsolicited block push, and relay networks. In addition to those techniques, we want to consider solutions considering the characteristics of VANET.

One possible solution to this issue is to decrease the message delivery delay between the good vehicles. We assume that RSUs are installed on the roads for V2I communications. All the RSUs are interconnected with each other using a wired network or optical fibers to guarantee low latency between them [41]. The vehicles can easily communicate with the RSUs using V2I communications. The end-to-end transmission delay between the good nodes can be reduced by utilizing wired connections between the RSUs. We assume that the RSUs will not be compromised easily. Even if some RSUs are compromised by the malicious vehicles, the number of RSUs compromised by the malicious vehicles will be small compared to the number of the legitimate RSUs. Thus, if the stability condition of (5) in Section V is satisfied by including RSUs in the good node group and by reducing the message delay using wired connections between RSUs, the regional blockchain might be safe from the immutability attack.

As another approach for reducing the message delivery delay between the good vehicles, we can consider applying cloud computing to the VANET. There were several research efforts at integrating cloud computing with VANETs. The vehicular cloud aggregates vehicular computing resources by interconnecting several vehicles in the cloud network [42]. Integrating the vehicles in the cloud enhances the computational capabilities, reliability, and scalability. It reduces delays that are crucial for exchanging the critical-event messages [43], [44], and solves some issues related with routing in V2V communications [45]. One issue with this approach is that if the nodes in the good vehicle group interconnect with each other using the cloud network for reduction of the message delivery delay, then the malicious vehicle group can use the same strategy to get connected to many malicious vehicles with a lower latency. In this case, the immutability attack may not be resolved efficiently.

As another application of the cloud, the RSUs can interconnect with each other and share their resources to form an RSU cloud to enhance computational capabilities with a low latency [46]. The RSU cloud hosts the computation services to meet the demand from the vehicles. If the vehicular clouds can be combined with RSU clouds, then the computing capability will have a synergy effect. In addition, the message delay between the good group nodes can be reduced. These approaches will be investigated further in future work.

## VIII. CONCLUSION

Regional blockchain is a blockchain shared among the members populated in a confined area. Since the area is limited, the message delivery time is reduced, and the puzzle computation time can be reduced as well. However, there was no previous work that suggests a guideline on the new puzzle computation time for this regional blockchain.

In this paper, we investigated how to design a secure regional blockchain for vehicular networks using several blockchain parameters. We showed that the puzzle computation time can affect the security of the blockchain especially in terms of the success probability of the 51% attack, which is also referred to as immutability attack in this paper. We derived a stability condition that guarantees a low immutability attack success probability in terms of the

number of good nodes, the number of malicious nodes, message delivery times, and the average puzzle computation time. We showed the validity of the stability condition through simulation, and investigated the effect of each control factor on the immutability attack success probability in detail. We found that the gap between the message delivery time of the good node group and that of the malicious group plays a very important role in the stability of the regional blockchain among the various control parameters. For example, 51% attack was possible even with a small ratio of malicious nodes, if the message delay for the malicious group is sufficiently shorter than that for the good node group. We also investigated a couple of ways to realize a low message delay among the good nodes in VANET qualitatively.

Our current analysis assumes that the initial chain depth, i.e. the depth of a block that the malicious group wants to forge, is sufficiently large for the stability of the blockchain system. The effect of the initial chain depth on the stability of the blockchain system has been investigated only through simulation in this work. The mathematical relation between the initial chain depth and the 51% attack success probability will be investigated further in our future work.

## APPENDIX

See Table 6.

**TABLE 6. Acronyms**

| Acronyms | Description |
|---|---|
| CA | Central Authority |
| IoT | Internet of Things |
| LIDAR | Light Detection and Ranging |
| OBU | On Board Unit |
| PoW | Proof of Work |
| PoS | Proof-of-Stake |
| PoC | Proof of Capacity |
| PBFT | Practical Byzantine Fault Tolerance |
| RSU | Road Side Unit |
| RoI | Region of Interest |
| V2X | Vehicle to Everything |
| V2I | Vehicle to Infrastructure |
| VANET | Vehicular Ad-hoc Network |
| HoL | Head-of-Line |
| ICD | Initial Chain Depth |

## REFERENCES

[1] H. Hartenstein and K. Laberteaux, *VANET: Vehicular Applications and Inter-Networking Technologies*, 1st ed. Hoboken, NJ, USA: Wiley, 2010.
[2] Research. (2018). *CBINSIGHTS*. Accessed: Jan. 18, 2019. [Online]. Available: https://www.cbinsights.com/research/autonomous-driverless-vehicles-corporations-list/
[3] Allied Market Research. (2018). *Autonomous Vehicle Market by Level of Automation*. Accessed: Dec. 10, 2018. [Online]. Available: https://www.alliedmarketresearch.com/autonomous-vehicle-market
[4] Wired.com. (2019). *Tesla's New Chip Holds the Key to 'Full Self-Driving'*. Accessed: Jul. 21, 2019. [Online]. Available: https://www.wired.com/story/teslas-new-chip-holds-key-full-self-driving/
[5] C. Li, W. Zhou, K. Yu, L. Fan, and J. Xia, "Enhanced secure transmission against intelligent attacks," *IEEE Access*, vol. 7, pp. 53596–53602, 2019.
[6] R. Shrestha and S. Y. Nam, "Trustworthy event-information dissemination in vehicular ad hoc networks," *Mobile Inf. Syst.*, vol. 2017, Nov. 2017, Art. no. 9050787.
[7] G. Martuscelli, A. Boukerche, and P. Bellavista, "Discovering traffic congestion along routes of interest using VANETs," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2013, pp. 528–533.
[8] A. P. Shrestha and K. S. Kwak, "Physical layer security in multiuser wireless networks," in *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention*. Hershey, PA, USA: IGI Global, 2017, pp. 263–281.
[9] A. Kchaou, R. Abassi, and S. Guemara, "Toward a distributed trust management scheme for VANET," in *Proc. 13th Int. Conf. Availability, Rel. Secur. (ARES)*, 2018, p. 53.
[10] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.
[11] J. A. Jaoude and R. G. Saade, "Blockchain applications—Usage in different domains," *IEEE Access*, vol. 7, pp. 45360–45381, 2019.
[12] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: www.bitcoin.org
[13] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Comput. Sci.-Res. Develop.*, vol. 33, nos. 1–2, pp. 207–214, 2018.
[14] X. Min, Q. Li, L. Liu, and L. Cui, "A Permissioned Blockchain Framework for supporting instant transaction and dynamic block size," in *Proc. IEEE 15th Int. Conf. Trust, Secur. Privacy Comput. Commun., IEEE 10th Int. Conf. Big Data Sci. Eng., IEEE 14th Int. Symp. Parallel Distrib. Process.*, Aug. 2016, pp. 90–96.
[15] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 2017, pp. 1–13, Aug. 2017.
[16] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 50–57, Oct. 2018.
[17] Z. Zheng, S. Xie, H. N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, pp. 352–375, 2018.
[18] A. M. Antonopoulos, *Mastering Bitcoin*, 1st ed. Newton, MA, USA: O'Reilly Media, 2015.
[19] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.
[20] B. Ostermaier, F. Dotzer, and M. Strassberger, "Enhancing the security of local DangerWarnings in VANETs—A simulative analysis of voting schemes," in *Proc. 2nd Int. Conf. Availability, Rel. Secur.*, Apr. 2007, pp. 422–431.
[21] J. Petit and Z. Mammeri, "Dynamic consensus for secured vehicular ad hoc networks," in *Proc. IEEE 7th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2011, pp. 1–8.
[22] A. Lei, C. Ogah, P. Asuquo, H. Cruickshank, and Z. Sun, "A secure key management scheme for heterogeneous secure vehicular communication systems," *ZTE Commun.*, vol. 21, pp. 1–11, Jun. 2016.
[23] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in *Proc. ACM Int. Jt. Conf. Pervasive Ubiquitous Comput. Adjun. (UbiComp)*, Jan. 2016, pp. 137–140.
[24] B. Leiding and W. V. Vorobev, "Enabling the vehicle economy using a blockchain-based value transaction layer protocol for vehicular ad-hoc networks," in *Proc. Medit. Conf. Inf. Syst. (MCIS)*, 2018, pp. 1–31.
[25] J. Rifkin, *The Third Industrial Revolution: How Lateral Power is Transforming Energy, the Economy, and the World*. London, U.K.: Palgrave Macmillan, 2011.
[26] D. Zhaoyang, L. Fengji, and G. Liang, "Blockchain: A secure, decentralized, trusted cyber infrastructure solution for future energy systems," *J. Modern Power Syst. Clean Energy*, vol. 6, no. 5, pp. 958–967, 2018.
[27] A. Giardina, "PROSUME: Decentralizing power," PROSUME, Milano, Italy, White Paper v2-2017, 2017.
[28] M. V. Kumar and N. C. S. N. Iyengar, "A framework for blockchain technology in Rice supply chain management," *Adv. Sci. Technol. Lett.*, vol. 146, pp. 125–130, Nov. 2017.
[29] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "FairAccess: A new Blockchain-based access control framework for the Internet of Things," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5943–5964, 2017.
[30] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," in *Proc. 13th IEEE Int. Conf. Peer-Peer Comput.*, Sep. 2013, pp. 1–10.

[31] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, vol. 16, pp. 3–16, Oct. 2016.
[32] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, "Consensus in the age of blockchains," 2017, *arXiv:1711.03936v2*. [Online]. Available: https://arxiv.org/abs/1711.03936v2
[33] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new-type of blockchain for secure message exchange in VANET," *Digit. Commun. Netw.*, vol. 2019, pp. 1–14, Apr. 2019.
[34] G. Salviotti, L. M. De Rossi, and N. Abbatemarco, "A structured framework to assess the business application landscape of blockchain technologies," in *Proc. 51st Hawaii Int. Conf. Syst. Sci.*, 2018, pp. 3467–3476.
[35] R. Shrestha, R. Bajracharya, and S. Y. Nam, "Blockchain-based message dissemination in VANET," in *Proc. IEEE 3rd Int. Conf. Comput., Commun. Secur.*, Oct. 2018, pp. 161–166.
[36] S. Y. Nikouei, R. Xu, D. Nagothu, Y. Chen, A. Aved, and E. Blasch, "Real-time index authentication for event-oriented surveillance video Query using blockchain," in *Proc. IEEE Int. Smart Cities Conf. (ISC)*, Sep. 2018, pp. 1–8.
[37] D. Zhang, H. Maei, X. Wang, and Y.-F. Wang, "Deep reinforcement learning for visual object tracking in videos," 2017, *arXiv:1701.08936*. [Online]. Available: https://arxiv.org/abs/1701.08936
[38] S. Kasahara and J. Kawahara, "Effect of Bitcoin fee on transaction-confirmation process," 2016, *arXiv:1604.00103*. [Online]. Available: https://arxiv.org/abs/1604.00103
[39] R. Bowden, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, "Block arrivals in the Bitcoin blockchain," 2018, *arXiv:1801.07447*. [Online]. Available: https://arxiv.org/abs/1801.07447
[40] R. W. Wolff, *Stochastic Modeling and the Theory of Queues*. Upper Saddle River, NJ, USA: Prentice-Hall, 1989.
[41] A. Mostafa, A. M. Vegni, R. Singoria, T. Oliveira, T. D. C. Little, and D. P. Agrawal, "A V2X-based approach for reduction of delay propagation in vehicular Ad-Hoc networks," in *Proc. 11th Int. Conf. ITS Telecommun. (ITST)*, Aug. 2011, pp. 756–761.
[42] S. Olariu, T. Hristov, and G. Yan, "The next paradigm shift: From vehicular networks to vehicular clouds," in *Mobile Ad Hoc Networking*. Hoboken, NJ, USA: Wiley, 2012, pp. 645–701.
[43] M. Abuelela and S. Olariu, "Taking VANET to the clouds," in *Proc. 8th Int. Conf. Adv. Mobile Comput. Multimedia (MoMM)*, 2010, pp. 6–13.
[44] R. Shrestha, R. Bajracharya, and S. Y. Nam, "Challenges of future VANET and cloud-based approaches," *Wireless Commun. Mobile Comput.*, vol. 2018, May 2018, Art. no. 5603518.
[45] Y. Qin, D. Huang, and X. Zhang, "VehiCloud: Cloud computing facilitating routing in vehicular networks," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 1438–1445.
[46] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, and S. Cherkaoui, "RSU cloud and its resource management in support of enhanced vehicular applications," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2014, pp. 127–132.

**RAKESH SHRESTHA** (M'19) received the B.E. degree in electronics and communication engineering from Tribhuwan University (TU), Nepal, in 2006, the M.E. degree in information and communication engineering from Chosun University, in 2010, and the Ph.D. degree in information and communication engineering from Yeungnam University, in 2018. From 2010 to 2011, he was a Security Engineer with Honeywell Security Systems. From 2010 to 2012, he was a Core Network Engineer with Huawei Technologies Company., Ltd., Nepal. From 2018 to 2019, he was a Postdoctoral Researcher with the Department of Information and Communication Engineering, Yeungnam University, South Korea. He is currently a Postdoctoral Researcher with the Yonsei Institute of Convergence Technology, Yonsei University. He was invited as a Keynote Speaker in the Third IEEE ICCCS Conference. His main research interests include wireless communications, mobile ad-hoc networks, vehicular ad-hoc networks, blockchain, the IoT, homomorphic encryption, deep learning, and wireless security. He was a Reviewer of several renowned journal and conferences.

**SEUNG YEOB NAM** (SM'14) received the B.S., M.S., and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 1997, 1999, and 2004, respectively. From 2004 to 2006, he was a Postdoctoral Research Fellow of the CyLab., Carnegie Mellon University. From 2006 to 2007, he was a Postdoctoral Researcher with the Department of Electrical Engineering and Computer Science, KAIST. In 2007, he joined the Department of Information and Communication Engineering, Yeungnam University, Gyeongsan, South Korea, where he is currently a Professor. His research interests include network security, network architecture, network management, and wireless networks. He received the Best Paper Award from the APCC 2000 Conference and the Bronze Prize from the 2004 Samsung Humantech Paper Contest.