IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 24, 2019, accepted May 20, 2019, date of publication May 22, 2019, date of current version June 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2918411

Impacts of Mobility on Performance of Blockchain in VANET

SEUNGMO KIM, (Member, IEEE)
Department of Electrical and Computer Engineering, Georgia Southern University, Statesboro, GA 30460, USA
e-mail: seungmokim@georgiasouthern.edu

This work was supported by the Georgia Southern University.

ABSTRACT This paper investigates how mobility affects the performance of a blockchain system operating in a vehicular ad hoc network (VANET). The mobility of nodes incurs a unique challenge to a blockchain system due to continuous change and dynamicity in the connectivity of the nodes. Specifically, the mobility makes a proof-of-work (PoW) process difficult since while moving the nodes can only have a limited length of time for a ''rendezvous'' to exchange a new block for verification. For this reason, accurate modeling for the block exchange behavior in a VANET is also challenging, which nevertheless has not been discussed in previous studies. Therefore, this paper provides an analysis framework that formulates the impact of mobility on a blockchain system's performance in a VANET based on three key metrics: (i) the probability of a successful addition of block to the chain; (ii) the stability of a rendezvous, and; (iii) the number of blocks exchanged during a rendezvous. The closed-form expressions and numerical results display the performance of a blockchain system in various scenarios in a VANET.

INDEX TERMS Blockchain, vehicular ad-hoc network (VANET), proof-of-work (PoW), full node (FN), rendezvous, number of exchanged blocks.

I. INTRODUCTION

A vehicular ad-hoc network (VANET) can improve the flow of traffic to facilitate intelligent transportation and to provide convenient information services. The goal of a VANET is to provide self-organizing data transmission capabilities for vehicles on the road to enable applications such as assisted vehicle driving and safety warnings [1]. Recently the European Parliament voted to adopt Dedicated Short-Range Communications (DSRC) instead of cellular vehicular-to-everything (C-V2X) [2], which supports that the 'infrastructure-less' VANET will provide a wider application in the near future.

Recently, various VANET applications have found potential value in this technology to promote accountability and credibility of the data [4]. Blockchain is a technology that leverages a distributed ledger to allow transactions between peers in a network, without the need for a central medium [3]. For instance, as vehicles become autonomous, they will increasingly need to exchange data with 'trust' in a variety of intelligent transportation scenarios such as smart contracts, which can benefit from application of the blockchain technology [5].

In a blockchain system, nodes do not trust each other and thus they run a 'validation' process whenever a new block is generated [3]. A node trusts a block only after completion of a consensus by running this validation process. It is called a proof-of-work (PoW) process, which provides a means to establish consensus on which a certain transaction is valid within the network. It is ideal if a block is validated by *all the full nodes (FNs)* in a network [6], which necessitates propagation of a block to all the FNs over an entire network. This makes a number of factors more significant than others in the performance of a blockchain network–*e.g.*, the number of nodes, total propagation delay, etc. Among them, this paper identifies *the number of nodes* in a blockchain network as a key factor since it consequently determines significant factors such as (i) the credibility and security of consensus via a PoW process [3] and (ii) the energy consumption level of a blockchain network [7].

The problem is that mobility of nodes in a VANET makes it complicated to accurately analyze the number of nodes that participate in propagation of a block. In fact, it is recently found that *unique tasks such as PoW and full blockchain*

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Fu Cheng.

validation cannot fully accurately work in a purely peer-to-peer VANET [8]. To elaborate, more than one FNs should physically come into each other's communication range in order to exchange a new block for PoW. However, since (i) there is no central infrastructure that can rely data exchange among nodes and (ii) the nodes are continuously moving, forming a "rendezvous" among blockchain nodes becomes especially challenging in a VANET. Provided this challenge, our natural interest then becomes to find answers for key questions: "how often a rendezvous can occur?"; "how long a rendezvous can last?"; and "how many blocks can be exchanged during a rendezvous?"

II. RELATED WORK

There is a body of recent work that studies application of blockchain in VANETs.

A. BLOCKCHAIN APPLIED TO VEHICULAR NETWORK

One body focuses on improvement of *security* and *credibility* in data exchanged in a VANET. A recent work proposes a three-layer architecture for ensuring security of data in a VANET [9]. Another latest work proposes a blockchain-based anonymous reputation system to break the linkability between real identities and public keys to preserve privacy [10]. There is also a paper that studies a consortium blockchain for secured data sharing and storage system in a VANET [11]. Another study uses consortium blockchain and smart contract technologies to achieve secured data storage and sharing in vehicular edge networks [17], which assumes that vehicular edge computing servers consisted of roadside units (RSUs) that cannot be fully trusted and thus may result in serious security and privacy challenges. Blockchain is applied to enhance edge computing for electric vehicles [12]: context-aware vehicular applications are identified according to the perspectives of information and energy interactions among electric vehicles, in which data contribution frequency and energy contribution amount are applied to achieve the PoW.

Another body shows interest in resolving *energy consumption* in a blockchain system that is applied to a vehicular network. A recent work shows a valuable insight on application of blockchain in a vehicular network [14]. Another latest work proposes a proof of trust consensus protocol to efficiently reach consensus among blockchain-operating electric vehicles, where the trust derivation is constructed based on the direct trust and credibility computing [13].

B. LIMITATIONS OF THE RELATED WORK

However, the prior work does not address the aforementioned unique challenge: a vehicular network is inherently mobile, which changes from an initial topology setup of a blockchain system and thus influences the retention of its initial consensus. Some prior work [14] suggested collection of 'partial' consensuses via clustering, yet it does not support the key idea of a blockchain's complete consensus. Hence, a fundamental question still remains unaddressed: how exactly one can evaluate impacts mobility of nodes a vehicular network on a blockchain's consensus performance?

Specifically, this paper points out two technical limitations in the current understanding:

First, no proper metric for a blockchain's performance exists. The current literature mostly focuses on credibility based on the detection theory [15] and the number of exchanged blocks [16] cannot accurately capture the impact of mobility on a blockchain in a vehicular network.

Second, no prior work discusses the 'imperfect' support of a vehicular network for a blockchain: recent discussions focus on security [17] [11] and forensic use [18] only, considering 100% support by a vehicular network for a blockchain, which is not practical nor realistic. Therefore, it must be found out how much a blockchain system's performance is affected by the nodes' mobility in a VANET.

TABLE 1. List of abbreviations and notations.

Abbreviations	
C-V2X	Cellular vehicle-to-everything
DSRC	Dedicated Short-Range Communications
FN	Full node
PoW	Proof of work
PPP	Poisson point process
RSU	Roadside unit
UAV	Unmanned aerial vehicle
V2X	Vehicle-to-everything
VANET	Vehicular ad-hoc network
Notations	
$\mathbb{A}_c$	Communication range for a FN of interest
$\mathcal{B}(t)$	Set of FNs forming in a rendezvous at time t
l	The length of the road segment
λ	Intensity of PPP: Number of nodes per unit area in $\mathbb{R}^2$
N_b	Number of blocks that can be exchanged during a rendezvous
n_{f}	Number of FNs forming a rendezvous at time t, $\mathbb{N}[\mathcal{B}(t)]$
n_c	Number of nodes competing for medium in an $\mathbb{A}_c$
p_s	Probability of a successful packet delivery
p_{sb}	Probability of a successful block exchange between FNs
$\mathbb{R}^2$	The two-dimensional road segment
r	Radius of a full node's communication range
ρ	The dynamicity
S	The stability of a 'rendezvous'
w	The width of the road segment

C. CONTRIBUTIONS

To the author's best knowledge, this paper is the first work to analyze the impacts of *mobility* on the performance of a blockchain system that is applied to a VANET.

The aforementioned limitations highlight the need for an accurate, comprehensive analytical framework to model the performance of a blockchain system affected by the nodes' mobility in a VANET. To this end, this paper presents the following unique contributions.

1) It considers a system model with complete generic two-dimensional movement of nodes, which can be generally applied to various VANET scenarios–*e.g.*, V2X, unmanned aerial vehicles (UAV), etc;
2) It formulates *the probability of a successful addition of block to the chain* as a metric that describes the impacts of nodes' mobility on the performance of a blockchain system;

3) As another metric, this paper provides a closed-form expression for *stability of a rendezvous*, which is defined as the time length while which two or more nodes can hold within each other's communication range.
4) As the third metric, it presents a closed-form formulation for *the number of blocks that can be exchanged* during a rendezvous. To demonstrate the relationship between the block generation interval (or 'block time'), this paper takes the Ethereum [25] as an example.
5) By incorporating all these components, this paper develops a *comprehensive analysis framework* that encompasses from modeling of nodes' mobility to analysis of the impacts of mobility on a blockchain system's performance.

III. SYSTEM MODEL

In the vehicular network model presented in this paper, a node is assumed to be mobile; for generality, a node can represent a vehicle, an UAV, and a pedestrian.

This paper adopts a completely distributed vehicular network, *i.e.*, VANET, in which no central coordinator node nor infrastructure (*e.g.*, server, spectrum access system [19], etc.) exists, in order to be loyal to the key pursuit of a blockchain system. This system model can generally suit currently operating VANET systems in practice including IEEE 802.11-based system such as DSRC and 802.11bd [20]. The model can also be applied to C-V2X as long as it operates directly among the nodes in a distributed manner, *e.g.*, sidelink-based broadcast or groupcast as defined in the 3rd Generation Partnership Project (3GPP) Release 16 [21].

Definition 1: A two-dimensional road segment $\mathbb{R}^2$ is defined with the length and width of l and w meters (m), respectively, as illustrated in Fig. 1. The southwest corner of $\mathbb{R}^2$ is defined as the origin, (0, 0).

Assumption 1: In order to capture a more dynamic and realistic movement of nodes in a vehicular network, this system model considers *no separation of lanes*, which makes itself more general than the system models that were provided in the previous work [22]–[24].

Assumption 2: In order to consider the most generic vehicle movement characteristic, this model assumes that any node moves in any direction, which enables the system to capture every possible movement scenario including flight of UAVs, lane changing, intersection, and pedestrian walking.

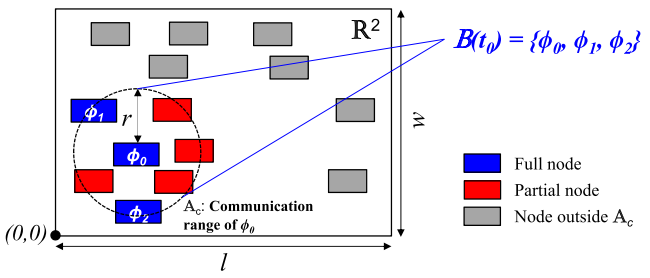


FIGURE 1. System geometry (An example captured at time instant t_0).

Assumption 3: The distribution of the nodes follows Poisson point process (PPP). This paper considers a two-tier VANET where the FNs and partial nodes are distributed in $\mathbb{R}^2$ according to independent homogeneous PPPs Φ_f and Φ_p with densities λ_f and λ_p, respectively. Therefore, a blockchain network is established over a total of $\mathbb{N}[\Phi_f] + \mathbb{N}[\Phi_p]$ nodes in the VANET. It also implies that *only a part of all the nodes in the network are equipped with the "full" capability* of generating, verifying, and broadcasting a new block, which are called "FNs." The other nodes are defined as "partial" nodes who are only able to 'receive' a block that is verified by one or more FNs.

Assumption 4: A VANET formed in $\mathbb{R}^2$ is 'fully connected.' Every node is supposed to be equipped with communication functionality and hence is able to broadcast it whenever a block has been generated.

Remark: When a new block is generated at a FN, it must be verified by another FN before being added to the chain. It means that a FN with the new block must *meet with at least one other FN* and hand the block to the other FN, in order to start a PoW process.

Definition 2: A *block exchange "rendezvous"* (a "rendezvous" hereafter) is defined as the physical geometry formed by more than one FNs such that they are placed within each other's communication range. Furthermore, a set of the FNs forming a rendezvous at time instant t_0 is denoted by $\mathcal{B}(t_0)$. Fig. 1 illustrates an example geometry. There are three FNs placed in each other's communication range, which yields $\mathcal{B}(t_0) = \{\phi_0, \phi_1, \phi_2\}$ where ϕ_i denotes the ith FN in set $\mathcal{B}(t_0)$.

Definition 3: The number of FNs that are forming a rendezvous at time instant t_0 is denoted as

$$n_f = \mathbb{N}[\mathcal{B}(t_0)]. \tag{1}$$

Remark: As already mentioned in Section I, an accurate validation of a new block is more likely as the number of FNs involved increases. In a blockchain system, nodes consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next PoW work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

Also, the rendezvous period, τ, can be longer if nodes move at a low velocity, whereas can be shorter if nodes move fast. The fundamental problem is "how many blocks can be exchanged during a rendezvous period?"

IV. ANALYSIS MODELS

The analysis framework presented in this paper focuses on the geometry for a "rendezvous" among n_f FNs where $n_f > 1$.

It starts with formulation of the probability that a block is successfully added to the chain during a rendezvous, as an indicator to measure the performance of a blockchain operating in a VANET. Then, the impact of mobility on a blockchain in a vehicular network is found.

A. PROBABILITY OF SUCCESSFUL BLOCK ADDITION TO THE CHAIN

Recall that the number of FNs forming a rendezvous, n_{f}, is an essential factor in a blockchain to determine the efficiency and energy efficiency in achieving a consensus in a blockchain. Further, due to nodes' mobility and dynamicity, it is even more critical to accurately measure n_{f} in a VANET.

Specifically, one should figure out *exactly how many FNs exist* in a road segment $\mathbb{R}^2$. It matters because as a larger number of FNs exist, a rendezvous can be formed more frequently, which again results in the higher verification and propagation capabilities for a blockchain network. Motivated from this necessity, this paper formulates the probability that an arbitrary node is a FN.

Assumption 5: Recall from *Assumption 3* in Section III that FNs are distributed following a PPP Φ_{f} with density of λ_{f}. Then the probability that there are n_{f} FNs in $\mathbb{R}^2$ can be formulated as

$$\mathbb{P}(n_{\mathrm{f}}|\lambda_{\mathrm{f}}) = \frac{(\lambda_{\mathrm{f}})^{n_{\mathrm{f}}}}{n_{\mathrm{f}}!} e^{-\lambda_{\mathrm{f}}}. \tag{2}$$

Definition 4: Hence, the probability that there are *at least two FNs* in $\mathbb{R}^2$ in order to form a rendezvous and exchange a block is formally written as

$$\begin{aligned} p_{\mathrm{f}} &= 1 - \mathbb{P}(0|\lambda_{\mathrm{f}}) - \mathbb{P}(1|\lambda_{\mathrm{f}}) \\ &= 1 - e^{-\lambda_{\mathrm{f}}}(1 + \lambda_{\mathrm{f}}). \end{aligned} \tag{3}$$

Definition 5: Then the *probability of a rendezvous* is defined as the probability that there are *at least two other FNs* in the communication range of an arbitrary FN, denoted by ϕ_i, which is given by

$$\begin{aligned} p_r &= p_{\mathrm{f}} \left(\frac{\mathbb{A}_c}{\mathbb{A}[\mathbb{R}^2]} \right)^2 \\ &= \frac{\pi r^2}{lw} \left[1 - e^{-\lambda_{\mathrm{f}}}(1 + \lambda_{\mathrm{f}}) \right] \end{aligned} \tag{4}$$

where $\mathbb{A}_c$ and $\mathbb{A}[\mathbb{R}^2]$ give the area of communication range for an arbitrary FN ϕ_i and the area of $\mathbb{R}^2$, respectively. Notice that although there can be more than two FNs forming a rendezvous, we maximize p_r by satisfying with a rendezvous formed by only two FNs, which is indicated by $\left(\mathbb{A}_c/\mathbb{A}[\mathbb{R}^2]\right)^2$.

Definition 6: The probability that a block generated at a FN is successfully delivered an arbitrary node on the blockchain is given by [24]

$$p_s(n_c) = \big(1 - p_{exp}(n_c)\big)\big(1 - p_{hn}(n_c)\big)\big(1 - p_{cs}(n_c)\big) \tag{5}$$

where n_c denotes the number of nodes located in the communication range of FN's, which follows another PPP and thus is given by

$$\begin{aligned} n_c &\approx \mathbb{E}[n_c] \\ &= \left(\lambda_p + \lambda_{\mathrm{f}}\right) \frac{\mathbb{A}_c}{\mathbb{A}[\mathbb{R}^2]} \\ &= \frac{\left(\lambda_p + \lambda_{\mathrm{f}}\right) \pi r^2}{lw}. \end{aligned} \tag{6}$$

Approximation of $n_c \approx \mathbb{E}[n_c]$ was introduced in a relevant prior study [24] on calculation of p_s.

The probabilities presented in (5) are elaborated as follows: (i) p_{exp} denotes the probability of a packet 'expiration' at the FN due to a backoff longer than 100 msec (the nominal average time length for a basic safety message (BSM) in DSRC, upon expiration of which the current one is discarded at the Tx and the next BSM is queued for transmission); (ii) p_{hn} gives the probability of a packet 'collision caused by a hidden node'; and (iii) p_{cs} is the probability of a packet 'collision caused by another node that happened to be allocated to same backoff coefficient' [24].

The probabilities, p_{exp}, p_{hn}, and p_{cs}, are 'numerically' found due to its formulation where an iterative method is needed, which repeats until the difference becomes smaller than 10^{-4} [24]. In fact, the method turned out to be effective in a previous work by this paper's author [22]. Appreciating the accuracy in obtaining the probabilities, this paper also relies on the same *numerical method* where iterations are run to find a sufficiently precisely approximated value for the number of nodes in a blockchain.

Theorem 1: As a consequence, based on (3) and (5), the probability that a block is successfully handed to another FN for verification can be formally written as

$$\begin{aligned} &p_{\mathrm{sb}}(\lambda_p, \lambda_{\mathrm{f}}, r, l, w) \\ &\quad = p_r p_s(\lambda_p + \lambda_{\mathrm{f}}) \\ &\quad = \frac{\pi r^2}{lw} \left[1 - e^{-\lambda_{\mathrm{f}}}(1 + \lambda_{\mathrm{f}}) \right] \big(1 - p_{exp}(\lambda_p + \lambda_{\mathrm{f}})\big) \\ &\qquad \times \big(1 - p_{hn}(\lambda_p + \lambda_{\mathrm{f}})\big)\big(1 - p_{cs}(\lambda_p + \lambda_{\mathrm{f}})\big). \end{aligned} \tag{7}$$

Demonstration of the numerical results for (7) are provided in Fig. 3 in Section V.

B. STABILITY: THE TIME LENGTH OF A RENDEZVOUS

Recall from *Definition 2* that a ''rendezvous'' is defined as a physical formation where two or more nodes are placed within each other's communication range. Not only the probability of a rendezvous, which is defined in (4), the time length of a rendezvous is also a critical factor in determining the performance of a blockchain network. The reason is that it can be further inferred to calculate the number of blocks that can be exchanged during a rendezvous, which will be discussed in Section IV-C.

Therefore, this subsection defines *the time length of a rendezvous* while $\mathbb{N}[\Phi_f]$ does not change, which will be also called the *stability of a rendezvous*. Accurate characterization of the stability is not trivial because a vehicular network is normally mobile, and further the nodes' mobility pattern itself

also keeps dynamic. Accounting the significance, a closed-form expression is derived for this new metric.

Lemma 1: Then the number of other FNs in an arbitrary FN ϕ_i's communication range at time instant $t_0 + \tau$ can be modeled as

$$\frac{n_{\mathrm{f}}\left(r-2v\tau\right)^2}{r^2} \leq n_{\mathrm{f}}^{\Delta}\left(v,\tau\right) \leq \frac{n_{\mathrm{f}}\left(r+2v\tau\right)^2}{r^2}. \tag{8}$$

where $n_{\mathrm{f}} = \lambda_{\mathrm{f}}\pi r^2$ since λ_{f} indicates the intensity of PPP for FNs, Φ_{f}, and πr^2 indicates the area of an arbitrary FN ϕ_i's communication range. A proof for this lemma is provided in Appendix A.

Definition 7: Based on (8), this paper classifies the use of (11) in the following two distinct cases:

$$Case1: \quad n_{\mathrm{f}} \leq n_{\mathrm{f}}^{\Delta}\left(v,\tau\right) \leq \frac{n_{\mathrm{f}}\left(r+2v\tau\right)^2}{r^2} \tag{9}$$

$$Case2: \quad \frac{n_{\mathrm{f}}\left(r-2v\tau\right)^2}{r^2} \leq n_{\mathrm{f}}^{\Delta}\left(v,\tau\right) < n_{\mathrm{f}} \tag{10}$$

representing two cases where the number of nodes has been 'increased' (Case 1) and 'decreased' (Case 2), respectively, as time passes from t_0 to $t_0 + \tau$.

Definition 8: The *dynamicity* of a blockchain network $\mathcal{B}$ is defined as the 'difference' in the number of nodes within the communication range of FN in a time duration of τ seconds, which is given by

$$\rho\left(v,\tau\right) = \frac{\left|n_{\mathrm{f}}^{\Delta}\left(v,\tau\right) - n_{\mathrm{f}}\right|}{\tau}, \tag{11}$$

where v gives the velocity of each vehicle. Notice that ρ is defined as a function of v and τ only, albeit it may also be affected by n_{f}.

Lemma 2: Considering (8), the dynamicity coefficient can be rewritten as

$$\rho\left(v,\tau\right) \leq \frac{n_{\mathrm{f}}\left(r+2v\tau\right)^2 - r^2 n_{\mathrm{f}}}{r^2\tau}, \quad Case1 \tag{12}$$

$$\rho\left(v,\tau\right) \geq \frac{r^2 n_{\mathrm{f}} - n_{\mathrm{f}}\left(r-2v\tau\right)^2}{r^2\tau}, \quad Case2 \tag{13}$$

Definition 9: Now, the *stability* of a vehicular network is defined as an inverse of the dynamicity, ρ. That is, the stability indicates a time length that is allowed for a blockchain to exchange a block until a consensus, in reference to a member node change. This quantity is formally written as

$$\begin{aligned}\mathsf{S}\left(v,\tau\right) &\equiv \rho^{-1}\left(v,\tau\right)\\ &= \frac{\tau}{\left|n_{\mathrm{f}}^{\Delta}\left(v,\tau\right) - n_{\mathrm{f}}\right|}.\end{aligned} \tag{14}$$

It is implied that $\mathsf{S}\left(v,\tau\right) = \infty$ when a blockchain operates in a 'fixed' network where no change in the number of nodes occurs, $n_{\mathrm{f}}^{\Delta}\left(v,\tau\right) = n_{\mathrm{f}}$.

One can also understand that S is modeled as a function of τ and v. The rationale is that as a vehicular network either (i) is observed for a longer time or (ii) moves faster, it gets more challenging for a blockchain to keep a consensus via exchanging a block all throughout the network. Furthermore, S is inversely proportional to $\left|n_{\mathrm{f}}^{\Delta}\left(v,\tau\right) - n_{\mathrm{f}}\right|$, which indicates that the rendezvous stability increases due to fewer nodes entering into or exiting from the network range.

Lemma 3: Plugging (12) into (14) leads to lower and upper bounds for the stability, S, which are given by

$$\mathsf{S}\left(v,\tau\right) \overset{(a)}{\geq} \frac{r^2}{4n_{\mathrm{f}}\left(v^2\tau + rv\right)}, \quad Case\ 1 \tag{15}$$

$$\mathsf{S}\left(v,\tau\right) \overset{(b)}{\leq} \frac{r^2}{-4n_{\mathrm{f}}\left(v^2\tau - rv\right)}, \quad Case2 \tag{16}$$

Notice in (a) and (b) that directions of the inequalities are switched during the inversion of $\mathsf{S} = \rho^{-1}$. Also, we suppose $r > v\tau$ in order to keep $\mathsf{S} > 0$ in (16), which means that we observe a node's movement, $v\tau$, only within the physical length of the FN's communication radius, r.

Theorem 2: When written in terms of v, the upper and lower bounds for S are given by

$$\begin{aligned}\mathsf{S}\left(v\right) &= \int_0^{\frac{r}{v}-\delta} \mathsf{S}\left(v,\tau\right) d\tau\\ &\geq \frac{r^2}{4n_{\mathrm{f}}v^2}\ln\left|\frac{2r - v\delta}{r}\right|, \quad Case1 \qquad (17)\\ &\leq -\frac{r^2}{4n_{\mathrm{f}}v^2}\ln\left|\frac{\delta v}{r}\right|, \quad Case2 \qquad (18)\end{aligned}$$

where δ denotes a sufficiently small number that is introduced to guarantee that $r > v\tau$. Specifically, we assume $0 \leq \tau \leq r/v - \delta$. A proof for the theorem is provided in Appendix B.

Theorem 3: Now, in terms of τ, the upper and lower bounds for S are formulated as

$$\begin{aligned}\mathsf{S}\left(\tau\right) &= \int_0^{\frac{r}{\tau}-\delta} \mathsf{S}\left(v,\tau\right) dv\\ &\geq \frac{r}{4n_{\mathrm{f}}}\left(\ln\left|\frac{\frac{r}{\tau}-\delta}{\delta}\right| + \frac{r}{\tau}\ln\left|\frac{2r-\delta\tau}{\delta\tau + r}\right|\right), \quad Case1 \qquad (19)\\ &\leq \frac{r}{4n_{\mathrm{f}}}\left(\ln\left|\frac{\frac{r}{\tau}-\delta}{\delta}\right| - \frac{r}{\tau}\ln\left|\frac{\delta}{-\delta\tau + r}\right|\right), \quad Case2 \qquad (20)\end{aligned}$$

A derivation for the integral is provided in Appendix C.

C. NUMBER OF BLOCKS EXCHANGED DURING A RENDEZVOUS

Theorem 4: Now, from *Lemma 3*, it is straightforward to calculate the range for *the number of blocks* that can be exchanged during a rendezvous as

$$\begin{aligned}N_b\left(v,\tau\right) &= \gamma\mathsf{S}\left(v,\tau\right)\\ &\geq \frac{\gamma r^2}{4n_{\mathrm{f}}\left(v^2\tau + rv\right)}, \quad Case1 \qquad (21)\\ &\leq \frac{\gamma r^2}{-4n_{\mathrm{f}}\left(v^2\tau - rv\right)}, \quad Case2 \qquad (22)\end{aligned}$$

where γ gives the number of blocks that are generated within a second. For instance, Bitcoin creates a block every 10 minutes, which yields $\gamma = 1/600\ \mathrm{sec}^{-1}$ [3] An average block

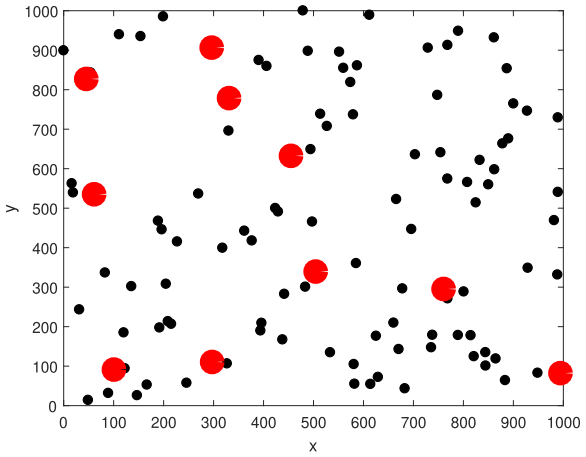


FIGURE 2. A snapshot of distribution of nodes ($l = w = 1$ km; partial nodes indicated by block dots with $\lambda_p = 100$ km^{-2} and FNs in red, larger circles with $\lambda_f = 10$ km^{-2}).

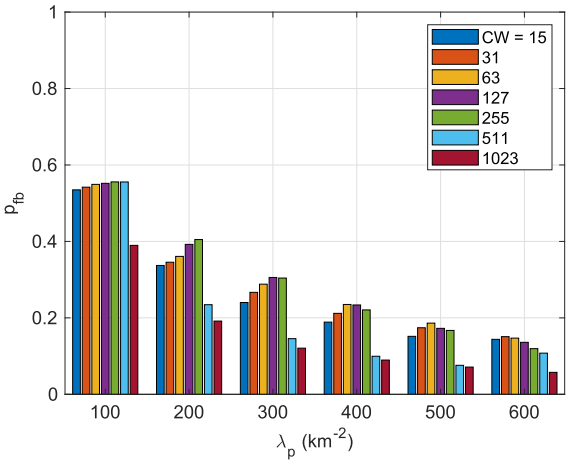


FIGURE 3. Probability of successful block exchange between at least two FNs according to number of nodes.

time for Ethereum is approximately 15 seconds, which gives $\gamma = 1/15$ sec^{-1} [25].

V. RESULTS

Now, numerical results for *Theorem 1* and demonstration of closed-form expressions of *Theorems 2* and *3* are evaluated. Dimension of the road segment $\mathbb{R}^2$ is given by $l = w = 1$ km. Also, recall that this paper supposes a distributed and asynchronous system to make suitable for establishment and operation of a blockchain in a 'distributed' fashion. Fig. 2 illustrates a snapshot for an example distribution of nodes.

A. PROBABILITY OF SUCCESSFUL BLOCK ADDITION TO THE CHAIN

As mentioned in Section IV-A, the probability of a successful packet delivery, p_s, is a key component of *Theorem 1* as it directly determines p_{sb}. Also recall that a *numerical* approach is taken to find p_s. The parameters that are used for the numerical computation are listed in Table 2.

TABLE 2. Parameters numerical computation of theorem 1.

Parameter	Value
System	IEEE 802.11p / DSRC
Slot time	66.7 μs
Inter-broadcast interval of BSM	100 msec
l	1 km
w	1 km
r	500 m
λ_f	10 km^{-2}
λ_p	{100, 200, 300, 400, 500, 600} km^{-2}

Fig. 3 demonstrates the probability that a block is successfully handed to another FN during a rendezvous, p_{sb}, versus the number of nodes within the node density, λ_p. Intuitively, a larger λ_p incurs a greater competition for the transmission medium, which yields a lower p_s. This leads to a decreasing tendency in p_{sb} as λ_p increases.

In order to evaluate a network's influence on the performance of a blockchain system, multiple values for maximum contention window (CW) are tested. Comparing the bars at each value for λ_p, a common pattern can be observed: an increase until an optimal value is reached; a zone where the reception probability remains constant; then a decrease follows. We can see that the optimal value of CW is smaller when the node density increases, which confirms the author's previous finding [22].

Rather than mathematically formulating this optimization problem, this paper describes the rationale as follows. Because p_s depends on both expirations and collisions, a balance must be found between the two types of failure. A packet expiration has the greatest impact on p_s, which is directly proportional to the CW size. This is due to packets being assigned backoff values that exceed the broadcast interval–*e.g.*, 100 msec for DSRC [26]. As a larger CW is selected, the number of collisions increases again due to more packets being transmitted without expiration. Additional increases in the CW result in a decreasing p_s due to additional packet collisions.

B. STABILITY OF NETWORK DURING A RENDEZVOUS

Fig. 4 plots the stability of a blockchain versus the velocity of a vehicle, $\mathsf{S}(v)$, given in *Theorem 2*. Although the analysis framework is general and thus other values could be used, as an example we assume $\lambda_p = 100$ km^{-2} in evaluation of $\mathsf{S}(v)$. From *Theorem 2*, it is intuitive that the stability of a blockchain is degraded as vehicles move faster, since it makes the number of nodes changes faster within a certain time length τ. Notice that the gap between Cases 1 and 2 gets wider as v increases. This can be explained in (27): with a larger v, differences among $\mathbf{x}_{(+)}$, $\mathbf{x}_{(-)}$, and $\mathbf{x}_{(=)}$ increase.

Fig. 5 shows the stability, $\mathsf{S}(\tau)$, versus the time duration during which a rendezvous is observed, τ. In contrast to the observation in Fig. 4, in this case $\mathsf{S}(\tau)$ for Cases 1 and 2

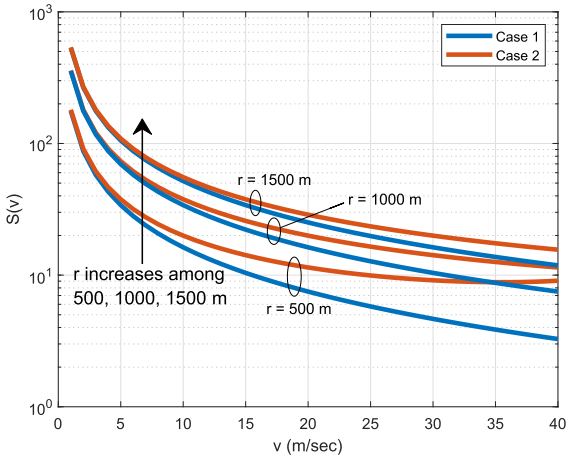


FIGURE 4. Stability of a rendezvous versus the velocity of nodes ($r = w = 1$ km, $\lambda_p = 100$ km^{-2}).

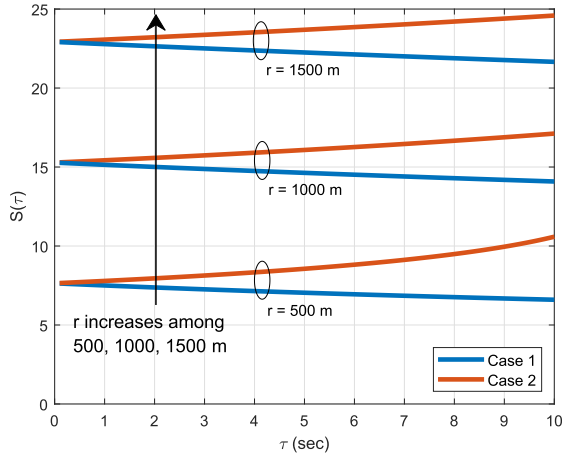


FIGURE 5. Stability of a rendezvous versus the rendezvous time ($r = w = 1$ km, $\lambda_p = 100$ km^{-2}).

diverge versus τ diverges according to the discussion. It confirms the intuition that as τ increases, the computational time for a blockchain consensus also increases. In addition, nodes are free to move in and out of the blockchain system due to long consensus times.

C. NUMBER OF BLOCKS EXCHANGED DURING A RENDEZVOUS

Fig. 6 demonstrates the number of blocks that can be exchanged while a rendezvous is formed versus the nodes' velocity, referring to *Theorem 4*. Notice that the plot shows an example for the Ethereum whose block time is 15 seconds. However, this analysis framework given in (21) and (22) can easily be extended to other blockchain systems whenever the value for γ is known. One can easily find that a slowly moving VANET can accommodate exchange of a larger number of blocks since it holds a rendezvous for a longer time. In the same sense, a larger r yields a greater N_b since a larger communication range for a FN leads to a longer rendezvous time period.

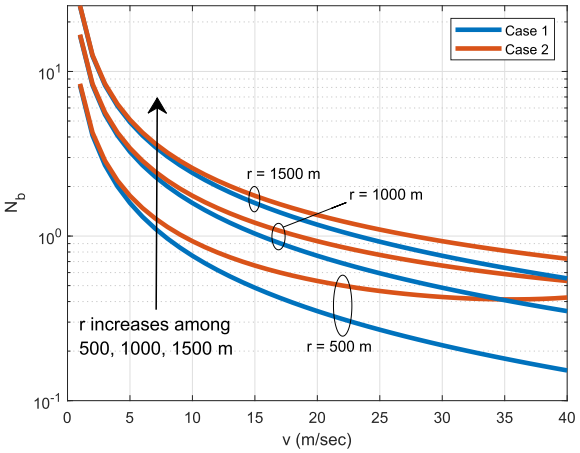


FIGURE 6. The number of blocks exchanged during a rendezvous (An example for Ethereum with $\gamma = 1/15$ sec^{-1} [25].

VI. CONCLUSION

While the blockchain technology has plenty of benefits, establishment of one in a VANET incurs challenges due to the nodes' mobility. To investigate the performance of a blockchain system applied to a VANET, this paper developed an analytical framework by using three metrics–(i) the probability of a successful addition of a block to the chain, (ii) the stability of a rendezvous, and (iii) the number of blocks exchanged during a rendezvous. Then the performance was evaluated via closed-form expressions and numerical solutions. Multiple key design insights were drawn from the results: (i) selection of CW has a significant influence on the probability of a successful block addition to the chain; (ii) the stability is determined by nodes' velocity, the number of FNs, and the radius of a FN's communication range; and (iii) the number of blocks that can be exchanged during a rendezvous can be inferred from the stability.

APPENDIX

A. PROOF OF LEMMA 1

Suppose that 'no vehicle collides': no other vehicle appears at the same position with another vehicle in t and $t+\tau$. However, the vehicles can move in any arbitrary direction.

When the FN is located at (x', y'), the set of points within the communication range $\mathcal{A}_c$ is defined as

$$\mathbf{c}(r) = \left\{(x, y) \middle| (x - x')^2 + (y - y')^2 \leq r^2\right\}. \qquad (23)$$

When it is assumed that every node in the road segment $\mathbb{R}^2$ moves at speed of v in arbitrary directions, after τ seconds, a farthest point from a point at the border of the circle given in (23) forms two other circles with the radius being $r + v\tau$ and $r - v\tau$. This forms an important conceptual basis for computation of ρ, the dynamicity of a vehicular network.

As illustrated in Fig. 7, at a time instant t_0, three distinct sets are defined–namely $\mathbf{x}_{(+)}$, $\mathbf{x}_{(-)}$, and $\mathbf{x}_{(=)}$, denoting a point

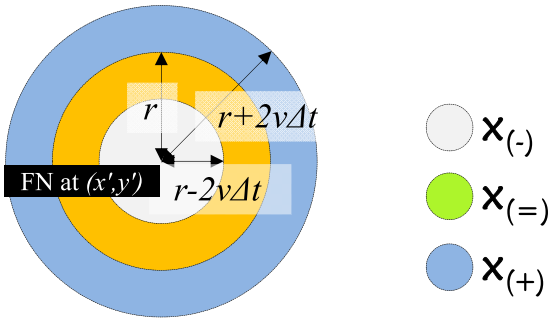


FIGURE 7. Sets $\mathbf{x}_{(+)}$, $\mathbf{x}_{(-)}$, and $\mathbf{x}_{(=)}$.

(x, y) on $\mathbb{R}^2$, being added to, taken out of, and staying in the network, respectively. The sets are formally written as

$$\mathbf{x}_{(+)} = \left\{(x, y) < \mathbf{c}\,(r + 2v\tau)^2 - \mathbf{c}\,(r)^2\right\} \tag{24}$$

$$\mathbf{x}_{(-)} = \left\{(x, y) > \mathbf{c}\,(r)^2 - \mathbf{c}\,(r - 2v\tau)^2\right\} \tag{25}$$

$$\mathbf{x}_{(=)} = \left\{(x, y) \leq \mathbf{c}\,(r - 2v\tau)^2\right\}. \tag{26}$$

Then the total number of nodes in the FN's communication range at time instant $t_0 + \tau$, denoted as n_{f}^{Δ}, comes into the following range. At minimum, all the nodes in the 'escapable' range, $\mathbf{x}_{(-)}$, get out while no node from the 'enterable' range, $\mathbf{x}_{(+)}$, newly comes in, and thus only those located in $\mathbf{x}_{(=)}$ stays in $\mathcal{B}(t_0 + \tau)$. Notice that a vehicle that was away by $r + 2v\tau$ can come into $\mathbf{x}_{(=)}$ when two vehicles move the exactly opposite directions with the same speed of v. At maximum, applying the similar logic, it is possible that no node in $\mathbf{x}_{(-)}$ escapes while every node in $\mathbf{x}_{(+)}$ is added, which thus only those located in $\mathbf{x}_{(=)}$ remain in the network $\mathcal{B}(t_0 + \tau)$. Now, using (23) through (26), n_{f}^{Δ} can be modeled as

$$\frac{n_{\mathrm{f}}\,(r - 2v\tau)^2}{r^2} \leq n_{\mathrm{f}}^{\Delta}\,(v, \tau) \leq \frac{n_{\mathrm{f}}\,(r + 2v\tau)^2}{r^2} \tag{27}$$

where $n_{\mathrm{f}} = \lambda_{\mathrm{f}}\pi r^2$.

B. PROOF OF THEOREM 2

The proof is based on the following integral:

$$\int \frac{c}{a\tau + b} d\tau = \frac{c}{a} \ln |a\tau + b| + C, \tag{28}$$

For **Case 1**, in order to derive (17), we apply the integral provided in (28) to (15), with the constants that are given by

$$a = 4n_{\mathrm{f}}v^2 \tag{29}$$

$$b = 4n_{\mathrm{f}}rv \tag{30}$$

$$c = r^2. \tag{31}$$

The integral is calculated as

$$\begin{aligned}
\mathsf{S}\,(v) &= \int_0^{\frac{r}{v}-\delta} \frac{c}{at + b} dt \\
&= \frac{c}{a}\Big[\ln |at + b|\Big]_0^{\frac{r}{v}-\delta} \\
&= \frac{c}{a}\left\{\ln \left|a\left(\frac{r}{v} - \delta\right) + b\right| - \ln |b|\right\} \\
&= \frac{r^2}{4n_{\mathrm{f}}v^2}\left\{\ln \left|4n_{\mathrm{f}}v^2\left(\frac{r}{v} - \delta\right) + 4n_{\mathrm{f}}rv\right| - \ln |4n_{\mathrm{f}}rv|\right\} \\
&= \frac{r^2}{4n_{\mathrm{f}}v^2}\left\{\ln \left|8n_{\mathrm{f}}rv - 4n_{\mathrm{f}}v^2\delta\right| - \ln |4n_{\mathrm{f}}rv|\right\} \\
&= \frac{r^2}{4n_{\mathrm{f}}v^2} \ln \left|\frac{8n_{\mathrm{f}}rv - 4n_{\mathrm{f}}v^2\delta}{4n_{\mathrm{f}}rv}\right| \\
&= \frac{r^2}{4n_{\mathrm{f}}v^2} \ln \left|\frac{2r - v\delta}{r}\right|
\end{aligned} \tag{32}$$

where δ is an arbitrary small number assigned for guaranteeing $\tau < \frac{r}{v}$, for which $\delta = 10^{-4}$ is used.

For **Case 2**, the following constants are substituted into (28):

$$a = -4n_{\mathrm{f}}v^2 \tag{33}$$

$$b = 4n_{\mathrm{f}}rv \tag{34}$$

$$c = r^2. \tag{35}$$

Application of the integral (28) to (16) leads to a derivation to (18), which is formally written as

$$\begin{aligned}
\mathsf{S}\,(v) &= \int_0^{\frac{r}{v}-\delta} \frac{c}{at + b} dt \\
&= \frac{c}{a}\Big[\ln |at + b|\Big]_0^{\frac{r}{v}-\delta} \\
&= \frac{c}{a}\left\{\ln \left|a\left(\frac{r}{v} - \delta\right) + b\right| - \ln |b|\right\} \\
&= \frac{r^2}{-4n_{\mathrm{f}}v^2}\left\{\ln \left|-4n_{\mathrm{f}}v^2\left(\frac{r}{v} - \delta\right) + 4n_{\mathrm{f}}rv\right| \right. \\
&\quad \left. - \ln |4n_{\mathrm{f}}rv|\right\} \\
&= -\frac{r^2}{4n_{\mathrm{f}}v^2}\left\{\ln \left|4n_{\mathrm{f}}v^2\delta\right| - \ln |4n_{\mathrm{f}}rv|\right\} \\
&= -\frac{r^2}{4n_{\mathrm{f}}v^2} \ln \left|\frac{4n_{\mathrm{f}}v^2\delta}{4n_{\mathrm{f}}rv}\right| \\
&= -\frac{r^2}{4n_{\mathrm{f}}v^2} \ln \left|\frac{\delta v}{r}\right|
\end{aligned} \tag{36}$$

C. PROOF OF THEOREM 3

In order to express S with respect to τ, one should integrate (15) and (16) in terms of v for Cases 1 and 2, respectively. Because both contain a second-order polynomial for v in the denominator, a partial fraction decomposition is applied, which is given by

$$\begin{aligned}
\frac{1}{av^2 + bv} &= \frac{A}{v} + \frac{B}{av + b} \\
&= \frac{(Aa + B)v + Ab}{av^2 + bv}
\end{aligned} \tag{37}$$

For **Case 1**, we derive (19) by applying (45) to integration of (15) in terms of v with the constants substituted by the

following values:

$$a = 4n_f\tau \tag{38}$$

$$b = 4n_f r \tag{39}$$

$$c = r^2. \tag{40}$$

To solve the simultaneous equations

$$\begin{aligned} Aa + B &= 0 \\ Ab &= 1 \\ A &= \frac{1}{b} = \frac{1}{4n_f r} \end{aligned} \tag{41}$$

$$Aa + B = a\frac{1}{b} + B = 0 \tag{42}$$

$$B = -\frac{a}{b} = -\frac{\tau}{r} \tag{43}$$

Integration of (37) leads to

$$\begin{aligned} \int \frac{c}{av^2 + bv} dv &= Ac \int \frac{1}{v} dv + Bc \int \frac{1}{av + b} dv \\ &= Ac \ln |v| + \frac{Bc}{a} \ln |av + b| + C, \end{aligned} \tag{44}$$

which again yields

$$\begin{aligned} &\int_0^{\frac{r}{\tau} - \delta} \frac{c}{av^2 + bv} dv \\ &= Ac \int_\delta^{\frac{r}{\tau} - \delta} \frac{1}{v} dv + Bc \int_\delta^{\frac{r}{\tau} - \delta} \frac{1}{av + b} dv \\ &= Ac \ln \left| \frac{\frac{r}{\tau} - \delta}{\delta} \right| + \frac{Bc}{a} \ln \left| \frac{a\left(\frac{r}{\tau} - \delta\right) + b}{a\delta + b} \right|. \end{aligned} \tag{45}$$

Therefore, integration with respect to v in order to express S in terms of τ:

$$\begin{aligned} &\int_\delta^{\frac{r}{\tau} - \delta} \frac{c}{av^2 + bv} dv \\ &= \frac{k}{b} \int_\delta^{\frac{r}{\tau} - \delta} \frac{1}{v} dv - \frac{ak}{b} \int_\delta^{\frac{r}{\tau} - \delta} \frac{1}{av + b} dv \\ &= \frac{c}{b} \left[\ln |v| \right]_\delta^{\frac{r}{\tau} - \delta} + \frac{c}{a} \left[\ln |av + b| \right]_\delta^{\frac{r}{\tau} - \delta} \\ &= \frac{c}{b} \left(\ln \left| \frac{r}{\tau} - \delta \right| - \ln |\delta| \right) \\ &\quad + \frac{c}{a} \left(\ln \left| a\left(\frac{r}{\tau} - \delta\right) + b \right| - \ln |a\delta + b| \right) \\ &= \frac{c}{b} \left(\ln \left| \frac{r}{\tau} - \delta \right| - \ln |\delta| \right] \\ &\quad + \frac{c}{a} \left(\ln \left| a\left(\frac{r}{\tau} - \delta\right) + b \right| - \ln |a\delta + b| \right) \\ &= \frac{c}{b} \ln \left| \frac{\frac{r}{\tau} - \delta}{\delta} \right| + \frac{c}{a} \ln \left| \frac{a\left(\frac{r}{\tau} - \delta\right) + b}{a\delta + b} \right|. \end{aligned} \tag{46}$$

It further leads to the lower bound for the stability as

$$\begin{aligned} \mathsf{S}(\tau) &\geq \frac{c}{b} \ln \left| \frac{\frac{r}{\tau} - \delta}{\delta} \right| + \frac{c}{a} \ln \left| \frac{a\left(\frac{r}{\tau} - \delta\right) + b}{a\delta + b} \right| \\ &= \frac{r^2}{4n_f r} \ln \left| \frac{\frac{r}{\tau} - \delta}{\delta} \right| + \frac{r^2}{4n_f \tau} \ln \left| \frac{4n_f\tau\left(\frac{r}{\tau} - \delta\right) + 4n_f r}{4n_f\tau\delta + 4n_f r} \right| \\ &= \frac{r^2}{4n_f r} \ln \left| \frac{\frac{r}{\tau} - \delta}{\delta} \right| + \frac{r^2}{4n_f \tau} \ln \left| \frac{\tau\left(\frac{r}{\tau} - \delta\right) + r}{\tau\delta + r} \right| \\ &= \frac{r}{4n_f} \ln \left| \frac{\frac{r}{\tau} - \delta}{\delta} \right| + \frac{r^2}{4n_f \tau} \ln \left| \frac{\tau\left(\frac{r}{\tau} - \delta\right) + r}{\tau\delta + r} \right| \\ &= \frac{r}{4n_f} \left(\ln \left| \frac{\frac{r}{\tau} - \delta}{\delta} \right| + \frac{r}{\tau} \ln \left| \frac{\tau\left(\frac{r}{\tau} - \delta\right) + r}{\tau\delta + r} \right| \right) \end{aligned} \tag{47}$$

For **Case 2**, we derive (20) by applying (45) to integration of (15) in terms of v with the constants substituted by the following values:

$$a = -4n_f\tau \tag{48}$$

$$b = 4n_f r \tag{49}$$

$$k = r^2. \tag{50}$$

Notice that the other constants in (45) are found as

$$A = \frac{1}{b} = \frac{1}{4n_f r} \tag{51}$$

$$B = -\frac{a}{b} = \frac{\tau}{r} \tag{52}$$

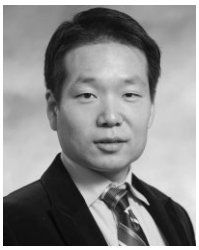
Then the closed-form expression for (20) can be finally obtained as

$$\begin{aligned} \mathsf{S}(\tau) &\leq \frac{k}{b} \ln \left| \frac{\frac{r}{\tau} - \delta}{\delta} \right| + \frac{k}{a} \ln \left| \frac{a\left(\frac{r}{\tau} - \delta\right) + b}{a\delta + b} \right| \\ &= \frac{r^2}{4n_f r} \ln \left| \frac{\frac{r}{\tau} - \delta}{\delta} \right| - \frac{r^2}{4n_f \tau} \ln \left| \frac{-4n_f\tau\left(\frac{r}{\tau} - \delta\right) + 4n_f r}{-4n_f\tau\delta + 4n_f r} \right| \\ &= \frac{r^2}{4n_f r} \ln \left| \frac{\frac{r}{\tau} - \delta}{\delta} \right| - \frac{r^2}{4n_f \tau} \ln \left| \frac{4n_f\delta}{-4n_f\tau\delta + 4n_f r} \right| \\ &= \frac{r}{4n_f} \ln \left| \frac{\frac{r}{\tau} - \delta}{\delta} \right| - \frac{r^2}{4n_f \tau} \ln \left| \frac{\delta}{-\tau\delta + r} \right| \\ &= \frac{r}{4n_f} \left(\ln \left| \frac{\frac{r}{\tau} - \delta}{\delta} \right| - \frac{r}{\tau} \ln \left| \frac{\delta}{-\tau\delta + r} \right| \right) \end{aligned} \tag{53}$$

REFERENCES

[1] E. C. Eze, S. Zhang, and E. Liu, "Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward," in *Proc. Int. Conf. Autom. Comput.*, Sep. 2014, pp. 176–181.
[2] J. van Roy, "EU parliament finally votes for WiFi to connect cars," *New Mobility News*, Apr. 2019. [Online]. Available: https://newmobility.news/2019/04/18/eu-parliament-finally-votes-for-wifi-to-connect-cars/
[3] S. Nakamoto. Oct. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[4] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commum. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[5] M. Singh and S. Kim, "Blockchain based intelligent vehicle data sharing framework," Jul. 2017, *arXiv:1708.09721*. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1708/1708.09721.pdf
[6] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," in *Proc. WEIS*, Jun. 2013, p. 11.
[7] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 1–28, Feb. 2018.
[8] M. Wagner and B. McMillin, "Cyber-physical transactions: A method for securing VANETs with blockchains," in *Proc. IEEE PRDC*, Dec. 2018, pp. 64–73.
[9] X. Zhang, R. Li, and B. Cui, "A security architecture of VANET based on blockchain and mobile edge computing," in *Proc. IEEE HotICN*, Aug. 2018, pp. 258–259.
[10] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in *Proc. IEEE TrustCom/BigDataSE*, Aug. 2018, pp. 98–103.
[11] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular adhoc network," *IEEE Access*, vol. 7, pp. 58241–58254, Jan. 2019.
[12] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, May/Jun. 2018.
[13] Y. Wang, Z. Su, and N. Zhang, "BSIS: Blockchain based secure incentive scheme for energy delivery in vehicular energy network," *IEEE Trans. Ind. Informat.*, to be published.
[14] V. Sharma, "An energy-efficient transaction model for the blockchain-enabled Internet of vehicles (IoV)," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 246–249, Feb. 2019.
[15] 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.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.
[16] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-based distributed framework for automotive industry in a smart city," *IEEE Trans. Ind. Informat.*, to be published.
[17] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, to be published.
[18] 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.
[19] M. Sohul, M. Yao, T. Yang, and J. H. Reed, "Spectrum access system for the citizen broadband radio service," *IEEE Commumn. Mag.*, vol. 53, no. 7, pp. 18–25, Jul. 2015.
[20] *Next Generation V2X (NGV) Study Group (SG)*, IEEE Standard 802.11, 2019. [Online]. Available: http://www.ieee802.org/11/Reports/tgbd_update.htm
[21] *Study on Enhancement of 3GPP Support for 5G V2X Services*, document 3GPP TR 22.886, 3GPP, (v16.2.0, Release 16), Dec. 2018.
[22] S. Kim and C. Dietrich, "A geometric analysis method for evaluation of coexistence between DSRC and Wi-Fi at 5.9 GHz," in *Proc. IEEE Globecom*, Dec. 2018, pp. 1–6.
[23] M. Farooq, H. ElSawy, and M. Alouini, "A stochastic geometry model for multi-hop highway vehicular communication," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2276–2291, Mar. 2016.
[24] R. Stanica, E. Chaput, and A. L. Beylot, "Reverse back-off mechanism for safety vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 16, pp. 210–224, May 2014.
[25] *Website for Etherchain—The Ethereum Blockchain Explorer*. Accessed: Mar. 20, 2019. [Online]. Available: https://www.etherchain.org/charts/blockTime
[26] K. A. Hafeez, A. Anpalagan, and L. Zhao, "Optimizing the control channel interval of the DSRC for vehicular safety applications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3377–3388, May 2015.



SEUNGMO KIM received the B.S. and M.S. degrees in electrical communications engineering from the Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 2006 and 2008, respectively, and the Ph.D. degree in electrical engineering from Virginia Tech., Blacksburg, VA, USA, in 2017. Since 2017, he has been an Assistant Professor with the Department of Electrical and Computer Engineering, Georgia Southern University, Statesboro, GA, USA. His current research interests include vehicle-to-everything (V2X) communications/networking, human exposure to electromagnetic field (EMF) in wireless systems, and the coexistence of 5G and IEEE 802.11 in the 60-GHz band. He was a recipient of the Best Paper Award from the IEEE WCNC 2016 International Workshop on Smart Spectrum. He is a member of the IEEE Communications Society.