Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment

Yao Sun, Lei Zhang, *Senior Member, IEEE*, Gang Feng, *Senior Member, IEEE*, Bowen Yang, Bin Cao, *Associate Member, IEEE*, and Muhammad Ali Imran, *Senior Member, IEEE*

***Abstract*—Blockchain has shown a great potential in Internet of Things (IoT) ecosystems for establishing trust and consensus mechanisms without involvement of any third party. Understanding the relationship between communication and blockchain as well as the performance constraints posing on the counterparts can facilitate designing a dedicated blockchain-enabled IoT systems. In this paper, we establish an analytical model for the blockchain-enabled wireless IoT system. By considering spatio-temporal domain Poisson distribution, i.e., node geographical distribution in spatial domain and transaction arrival rate in time domain are both modeled as Poisson point process (PPP), we first derive the distribution of signal-to-interference-plus-noise ratio (SINR), blockchain transaction successful rate as well as overall throughput. Based on the system model and performance analysis, we design an algorithm to determine the optimal full function node deployment for blockchain system under the criterion of maximizing transaction throughput. Finally, the security performance is analyzed in the proposed networks with three typical attacks. Solutions such as physical layer security are presented and discussed to keep the system secure under these attacks. Numerical results validate the accuracy of our theoretical analysis and optimal node deployment algorithm.**

***Index Terms*—Blockchain, consensus mechanism, Internet of Things (IoT), node deployment, security performance analysis, transaction throughput.**

I. Introduction

INTERNET of Things (IoT) is envisioned as one of the most promising technologies for constructing a global network with machines and devices which will gradually cover almost all aspects of the human life [1], [2]. With such an important role it plays in our life, there is a consensus that the security problem is of the first priority of IoT [3], [4], due to the easy accessibility and hardware/software constraints on IoT devices. Thus, tremendous effort and cost need to be invested to update these devices once any vulnerability is detected. Moreover, in the current centralized IoT system, a cloud server is necessary for the identification, authorization, and communication among low-end devices, resulting in huge expenditure on construction and maintenance of servers. Finally, in the centralized IoT system, due to the involvement of the third party, the high agent cost makes smart contract [5] (such as micro payment and information exchange) among devices unattractive, and thus poses a bottleneck on the prosperous of IoT ecosystems.

A. Preliminaries: Blockchain

In order to effectively address the aforementioned problems, intensive work has been done. As a revolution in systems of record, blockchain has been regarded as a promising technology to address IoT's trust and security concerns, as well as high maintenance cost problem [5], [6]. Proof of work (PoW)-based blockchain is the underling technique of Bitcoin, which has became a revolutionary decentralized data management framework. For example, in the application of stipulating smart contracts, the contract is stored and updated by devices themselves on chains, which are created and broadcast by those users authorized by a consensus mechanism. The blockchain is formed by a continuously growing set of data blocks, and each data block is generated by processing the transaction information with certain cryptography algorithms [7]. The main principles underlying the blockchain are summarized as follows [8], [9].

1) The transactions happen directly between peers instead of through a central server, and each transaction information will be forwarded to all other nodes.
2) Each node within the blockchain has the right to access to the entire database, and contribute to the calculation and verification of the new block generated by the collected transactions.

Manuscript received November 19, 2018; revised February 28, 2019; accepted March 12, 2019. Date of publication March 18, 2019; date of current version June 19, 2019. This work was supported in part by the National Science Foundation of China under Grant 61631004 and Grant 61971099 and in part by the U.K. Engineering and Physical Science Research Council under Grant EP/S02647X/01. *(Corresponding author: Lei Zhang.)*

Y. Sun and G. Feng are with the National Key Laboratory on Communications, University of Electronic Science and Technology of China, Chengdu 610051, China, and also with the Center for Intelligent Networking and Communications, University of Electronic Science and Technology of China, Chengdu 610051, China (e-mail: sunyao@std.uestc.edu.cn; fenggang@uestc.edu.cn).

L. Zhang, B. Yang, and M. A. Imran are with the School of Engineering, University of Glasgow, Glasgow G12 8QQ, U.K. (e-mail: lei.zhang@glasgow.ac.uk; b.yang.1@research.gla.ac.uk; muhammad.imran@glasgow.ac.uk).

B. Cao is with the Institute of Network Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: caobin65@163.com).

Digital Object Identifier 10.1109/JIOT.2019.2905743

3) Various cryptography algorithms and consensus mechanisms[1] are implemented to guarantee the records in the database. It is extremely difficult for any single party to tamper or delete the records as they are correlated to every transaction record came before them.
4) The system is secure as long as a certain percentage of CPU power (for example 51% in PoW system) within the system is not controlled by any cooperating group of attacker nodes.

Because of the above features, blockchain technique enables the progress and cost effective, highly safe transaction, which is exactly the missing part of the current IoT ecosystems. Specifically, blockchain allows the secured and reliable transactions/communications between two smart devices without the need of centralized authority, which improves the settlement time from days to almost instantaneous [12] apart from saving agent fees. As such, international data cooperation (IDC) forecasts that around 20% of the deployed IoT systems will enable basic blockchain services in 2019 [13].

B. Motivations

Although good prospects can be expected, there are some problems associated with the combination of blockchain and IoT. As pointed by [5], it is computationally intensive and power consuming to implement the current blockchain technique (especially PoW-based one), but most of the IoT devices may not bear the necessary computing capability, memory space as well as power supplement to run and store blockchain. Relevant state-of-the-art work focuses on the blockchain protocols design in terms of consensus mechanism [5], [10], [11], trust and privacy [7], [8], etc. while no more consideration on an efficient network architecture to support low cost blockchain-enabled wireless IoT system. Only the authors in work [14] propose a blockchain-enabled IoT network architecture with requirement of central management which is more suitable for a small local network (such as smart home in that paper).

From the communication perspective, in the traditional blockchain systems, a common assumption is that communications among the nodes are perfect without any throughput and delay constraints. However, considering the unstable channel quality, interference, limited resource, and various network topology, it is necessary to investigate the impact of wireless communication on the overall blockchain-enabled IoT system. In particular, some fundamental metrics, such as signal-to-interference-plus-noise ratio (SINR) and throughput should be analyzed to show how the wireless communication quality may affect/constrain the blockchain-enabled IoT network deployment (e.g., node distribution), protocols (e.g., size of block and frequency of transactions) and transaction consensus delay, etc. On the other hand, given a transaction throughout bound in blockchain (e.g., one block in every 10 min as defined in Bitcoin [15]), it is valuable to know how to deploy the IoT nodes that can optimally meet this bound. In general, the performance of blockchain-enabled IoT system in terms of transaction throughput (the number of confirmed transactions in a unit time), communication throughput (the amount of transmitted data in a unit time), transaction successful rate should be associated with both blockchain transaction arrival rate in time domain and nodes geographic distribution in spatial domain. Therefore, a fundamental challenge is that how to establish a valid framework of analytical model considering the 2-D randomness to evaluate the performance of blockchain-enabled IoT system.

Although there has been tremendous research work on wireless network modeling, the existing performance analysis focusing on traditional wireless networks cannot be directly applied to blockchain-enabled IoT system due to the lack consideration of blockchains. Work [16]–[18] exploit stochastic geometry to evaluate the network performance in terms of association probability, throughput and outage probability, for traditional cellular networks [16], heterogeneous cellular networks [17], and millimeter wave networks [18], respectively. These investigations focus on spatial domain without the consideration of time domain whose characteristics are much different for blockchains. Most existing work that simultaneously considers spatial and time domains, such as [19]–[21], combining queueing theory and stochastic geometry to evaluate delay performance. However, considering the characteristics of blockchain (e.g., low transaction arrival rate and limited transaction throughput), the performance evaluations could be much different.

In addition to communication performance analysis for block-enabled IoT system, security performance analysis is also necessary when some attacks exist in this system. Considering the vulnerable wireless links, the types of attacks could be various. To the best of the authors' knowledge, there is no such analytical models dedicated to blockchain-enabled wireless IoT systems.

C. Contributions and Organizations

In this paper, we first present a new network model for blockchain-enabled IoT system. Then, we theoretically analyze the performance of the blockchain-enabled IoT system, and propose an optimal blockchain full function node (FN)[2] deployment based on the analysis. Numerical results show that the difference between analytical and simulation results is as low as 4%, which clearly validate the accuracy of our theoretical analysis. The main contributions of this paper can be summarized as follows.

1) We present a blockchain-enabled wireless IoT system model, where some full FNs are deployed to fulfill the functions of blockchain thus to support the transactions between other low-end IoT devices. Moreover, we clarify the two key concepts in blockchain-enabled IoT networks: a) blockchain transaction throughput and communication throughput and b) derive the mathematical relationship between them.

[1]Except the most commonly used PoW-based consensus mechanism, many other lower computational complexity mechanisms are proposed, such as proof of stake (PoS) based [10] and direct acyclic graph (DAG) based [11] blockchains. However, the framework proposed in this paper can underpin all these blockchain consensus mechanisms. In this paper, we will take PoW-based mechanism as an example.

[2]Full FN has high computing and storage power with full functionalities to support blockchain protocols, which will be explained in detail in Section II.

2) We theoretically analyze the performance of blockchain-enabled IoT system. In detail, considering the spatio-temporal domain Poisson point process (PPP) modeling, i.e., node geographical distribution and transaction arrival rate in time domain, we derive the probability density function (PDF) of SINR for a transmission from an IoT node to a full FN. Accordingly, the transaction successful rate and overall communication throughput are analytically calculated.
3) Given the derived analytical model, a searching algorithm is proposed to find the optimal blockchain full FN deployment under a given IoT node density and blockchain transaction throughput.
4) The security performance is analyzed in the proposed system with three typical kinds of attacks, i.e., eclipse attack, random link attack, and random node attack. Solutions, such as physical layer security are presented and discussed to keep the system secure under such attacks. Simulation results show that under these attacks, the proposed system model is still valid.

The rest of this paper is organized as follows. In Section II, we present the system model for blockchain-enabled wireless IoT networks. In Section III, we theoretically analyze the performance of blockchains in IoT systems. Then, we propose an optimal blockchain full FN deployment in Section IV based on the performance analysis. The security performance analysis is presented in Section V. In Section VI, we present the numerical results. Finally, Section VII concludes this paper.

II. System Model

In this section, we first present the blockchain-enabled IoT network model, and then describe the wireless communication model by considering the spatio-temporal domain characteristics of this network.

A. Blockchain-Enabled IoT Network Model

Consider a blockchain-enabled IoT network shown in Fig. 1, which consists of two main elements: 1) IoT transaction nodes (TNs) and 2) full FNs. TNs can be basically seen as traditional low-cost low-power IoT devices supported by blockchain system. At any time point, the TNs can be classified as two types: 1) active TNs with data being transmitted and 2) idle TNs with no transmissions. Note that the two states of a TN can be switched. The detailed time domain characteristics will be further discussed in the next section. FNs are the nodes in blockchain with high computing and storage power. They have full functionalities to support blockchain protocols thus to take charge of transaction confirmation, data storage, and building new blocks. To guarantee the security and improve the effectiveness in blockchain, FNs are connected with each other through high data rate links via independent interface. In addition, all FNs connect with TNs through wireless communications. Transactions can be seen as any valuable information transmitted between TNs. They are confirmed by FNs, and stored in blocks.

A transaction process can be described as follows. Once a transaction arrives to a specific TN, the TN should broadcast the information to FNs by using wireless IoT networks. This

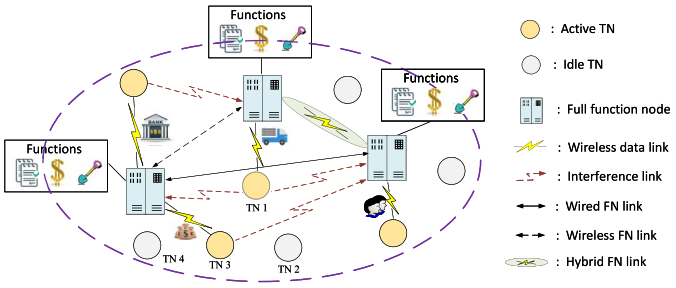


Fig. 1. Blockchain-enabled IoT network model.

information should be received by as many FNs as possible to enhance the security level, however, in this paper, as a starting point, we assume that each transaction successfully received by a single FN is secure. Nevertheless, our analysis framework can be generalized to the scenario where each transaction should be successfully received by multiple FNs. The received information by an FN through wireless channel will be shared within all FNs via the dedicated connections. Then, the FN which has the right of building a block will insert this transaction into the chain, and all FNs need to update their own ledger accordingly. Note that our focus in this paper is uplink transmission from TN to FN. While the downlink performance analysis can be performed in a similar manner, which is out of the scope of this paper.

The association relationship between TNs and FNs is not fixed. More specifically, Fig. 1 presents an instantaneous network state at a certain time. Note that the network state, including the active TNs, the active FNs, the association relationship between TNs and FNs, etc. can be dynamic along with time. In other word, TNs can choose a suitable FN to be served according to current network state (in this paper, we assume that TNs choose the nearest trust-able FN). Please note that the FN set and some nodes in the TN set can dynamically switch depending on the needs. In the case of an FN is shut down or attacked, the TNs which are associated with this FN can be associated with other nearby trust-able FNs. Therefore, the centralization problem can be avoided in our system.

We assume that some malicious FN nodes exist in the network, and the percentage of the malicious FN nodes do not exceed the half thus does not violate the security requirement of blockchain system. Also, the malicious FNs can make denial of service (DoS) attack (e.g., reject to forward). In this case, it is equivalent to the FNs are shut down, and the TNs associated with them will seek for other nearby FNs. However, the malicious FNs cannot change the transaction since it is authenticated by digital signature [22]. If any part of the transaction is modified by the malicious FN, the signature would be invalidated, thus this transaction cannot be inserted into a block. As a result, the TN will seek for other nearby FNs when the transaction is not confirmed within predefined duration. In this case, mathematically, it is equivalent to the case of FN is shut down as well.

We assume that the connection between FNs can be several types, including wired link, wireless point to point link, and wired and wireless hybrid relay link, as shown in Fig. 1. The connection type between two specific FNs is determined by

the environment around the two FNs. For example, traditional wireless link can be used when the distance between the two FNs is short, while wired link should be used in the complicated environment. Moreover, for the large scale IoT networks, the wired-wireless hybrid connections could be more practical and cost effective.

Before moving to wireless communication model, we need to clarify two definitions in blockchain-enabled IoT networks: 1) transaction throughput and 2) communication throughput. Transaction throughput is defined as the number of transactions confirmed in a unit time by the blockchain system. Usually, we use transactions per second (TPS) as the metric. In communication unlimited case without delay and throughput constraints, TPS is typically limited by the block size, consensus mechanism as well as the transaction arrival rate. For example, the maximum TPS of Bitcoin and Ethereum is 7 and 20, respectively [23]. Communication throughput is defined as the amount of transmitted data in a unit time for this network. Usually, we use bits per second (bps) as the unit. It is related to wireless channel condition, radio resource allocation as well as radio access technology [e.g., long term evolution (LTE) and WiFi]. In the wireless blockchain networks, the required communication throughput R can be calculated based on the transaction throughput C_T as follows:

$$R \geq LC_T \tag{1}$$

where L is the packet length for a transaction. As the limitation of C_T, there is a maximum required communication throughput.

B. Wireless Communication Model

We present the wireless communication model with respect to the spatio-temporal domain characteristics of blockchain-enabled IoT networks. We first describe the network spatial distribution. Let A be the considered 2-D area where TNs and FNs are assumed to be distributed as a homogeneous PPP with density λ_d and λ_f, respectively. It is practical to assume that the minimum distance between a TN and an FN is set as $d_{\min}$. The association rule between TNs and FNs is based on distance, i.e., a TN is associated with the nearest FN.

Then, we describe the time domain characteristics of blockchain-enabled IoT networks. For a specific TN, once a transaction arrives, the TN should be in active mode to broadcast the information to FNs. Fig. 2 shows the time domain characteristics for a case of 4 TNs in Fig. 1, where we find that at time t_1, TN 1 and TN 3 are active, and thus TN 3 could generate interference to TN 1 and vice verse; while at time t_2, TN 2, 3, and 4 interfere with each other. The transaction packet length L is usually very short. In 3GPP Standard, the data packet size (i.e., active time of TN) can be modeled as Pareto distribution with shape parameter alpha = 2.5 and minimum data packet size = 20 bytes [24]. Therefore, the expectation of the data packet size in IoT network is around 33.3 bytes, which can be transmitted in a single transmission time interval (TTI) in 1 ms by using LTE system [25]. Moreover, the traffic arrival rate is as low as from half an hour to even several hours [24], implying that the traffic of IoT nodes is not very active. Hence, based on the above two reasons, it is reasonable to assume that the TNs active time is a small constant

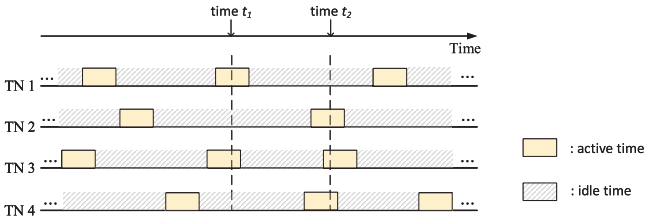


Fig. 2. Arrival traffic of TNs in time domain.

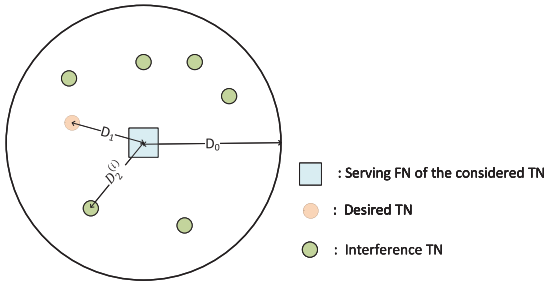


Fig. 3. Interference area for a specific TN.

with $t \ll T$, and thus the number of arrived transactions M in time T can be assumed to be a Poisson distribution with parameter $\lambda_a T$.

For the wireless channel, as mentioned in Section II-A, we focus on uplink transmission in this paper. Consider a specific TN served by an FN, the desired signals experience path loss $g(d)$ where d is the distance between the TN and the FN. Define interference TN as the TNs that generate interference to the considered TN. Obviously, from the time domain, as indicated in Fig. 2, only the active TNs could be counted as interference TNs. In addition, from the spatial domain, we assume only the TNs within a certain circular area, where the serving FN is located as the center with radius D_0 as shown in Fig. 3, could contribute to the interference. We set the transmit power of all TNs as P. Therefore, the received SINR can be expressed as

$$\mathrm{SINR}(D_1, N_I, \mathbf{D}_2) = \frac{Pg(D_1)}{\sum_{i=1}^{N_I} Pg\left(D_2^{(i)}\right) + \sigma} \tag{2}$$

where D_1 is the distance between the desired TN and the serving FN, $\mathbf{D}_2 = [D_2^{(1)}, D_2^{(2)}, \ldots, D_2^{(N_I)}]$ is the distance vector for all interference TNs, N_I is the number of interference TNs, and σ is the noise power. Denote β as the SINR threshold that FNs can successfully decode the received information bits. For convenience, the frequently used notations are summarized in Table I.

III. Performance Analysis in Blockchain-Enabled Wireless IoT Networks

In this section, we theoretically analyze the transmission performance in terms of SINR, transaction data packet (TDP) transmission successful rate as well as overall communication throughput by considering the blockchain characteristics, such as short transaction packet length, low TN active rate, and limited transaction throughput. In detail, we first derive the PDF of SINR according to the spatio-temporal domain modeling,

TABLE I
FREQUENTLY USED NOTATIONS

Notation	Definition
A	the whole considered area
D_0	radius of interference area
D_1	distance between desired TN and the serving FN
$\mathbf{D}_2$	distance vector of all interference UEs (a vector)
$D_2^{(i)}$	distance between interference TN i and the FN
λ_d	TN density
λ_f	FN density
λ_a	blockchain transaction arrival rate
M_i	number of arrival transactions in time T for TN i
N_0	the number of total TNs
K	the number of TNs in interference area
N_I	the number of interference TNs
t	radio transmission time for a transaction
T	the total considered time
L	the packet length of each blockchain transaction
P	TN transmit power
$g(d)$	channel path loss model (a function of distance)
f_X	probability density function of random variable X

and then calculate the blockchain TDP transmission successful rate based on the PDF of SINR. Finally, we obtain the PDF of overall communication throughput in a close-form expression under the constraints of blockchain transaction throughput and the TDP transmission successful rate.

A. Probability Density Function of SINR

Let us start with SINR distribution analysis. As both TNs and FNs are geographically distributed as homogeneous PPP, it is reasonable to investigate the SINR performance of any an arbitrary TN. To derive the PDF of SINR in (2), the desired signal power and interference need to be studied separately.

For a specific TN, the desired signal power S is a random variable written as $S = Pg(D_1)$, where D_1 is the distance between the TN and the serving FN. As transmit power P is fixed in this paper, S is only related to D_1. Proposition 1 gives the PDF of D_1. For convenience, we use capital letters to denote random variables, and the corresponding lowercases to the value of random variables.

Proposition 1: The PDF of the distance D_1 between a specific TN and the serving FN is

$$f_{D_1}(d_1) = 2\pi\lambda_f d_1 \exp\{-\lambda_f \pi (d_1)^2\}. \tag{3}$$

Proof: According to the association rules presented in Section II, $D_1 > d_1$ is the event that there is no FN distributed in the circular area with radius d_1. Thus, $\Pr(D_1 > d_1) = \exp\{-\lambda_f \pi (d_1)^2\}$. Hence, the PDF of D_1 is $f_{D_1}(d_1) = [d(F_{D_1}(d_1))]/d(d_1) = 2\pi\lambda_f d_1 \exp\{-\lambda_f \pi (d_1)^2\}$. ■

Therefore, based on Proposition 1, we obtain that the PDF of desired signal power as

$$f_S\big(S = Pg(d_1)\big) = f_{D_1}(d_1) = 2\pi\lambda_f d_1 \exp\{-\lambda_f \pi (d_1)^2\}. \tag{4}$$

We now study the distribution of the received interference. We start from the number of interference TNs N_I. As stated in Section II, only active TNs located in the interference area will be counted for interference contribution.[3] The number of TNs $K (K \geq N_I)$ within the interference area is still a variable of Poisson distribution with density parameter $\pi (D_0)^2 \lambda_d$. On the other hand, as the transmission time for TN is t, the TNs which are active during time period $[-t, t]$ can bring interference. For a TN, the number of arrived transactions is distributed as PPP with parameter $2t\lambda_a$. Therefore, the active probability for a TN during time period $[-t, t]$ is

$$\Pr(\text{active}) = 1 - \exp\{-2t\lambda_a\}. \tag{5}$$

The probability of the number of interference TNs $N_I = n_I$ given $K = k$ is

$$\Pr(N_I = n_I | K = k) = C_k^{n_I} (1 - \exp\{-2t\lambda_a\})^{n_I} \tag{6}$$

where $C_k^{n_I}$ is the combinational number. Therefore, the PDF of N_I is

$$\begin{aligned} f_{N_I}(n_I) &= \Pr(N_I = n_I) \\ &= \sum_{k=n_I}^{N_0} \Pr(N_I = n_I | K = k) \Pr(K = k) \end{aligned} \tag{7}$$

where

$$\Pr(K = k) = \frac{(\pi (D_0)^2 \lambda_d)^k}{k!} \exp\{-\pi (D_0)^2 \lambda_d\}. \tag{8}$$

Then, we investigate the distance $D_2^{(i)}$ between an interference TN i and the FN. Proposition 2 gives the PDF of $D_2^{(i)}$.

Proposition 2: The PDF of the distance D_2 is

$$f_{D_2^{(i)}}(d_2^{(i)}) = \frac{2d_2^{(i)}}{(D_0)^2} \tag{9}$$

where D_0 is the radius of the interference area.

Proof: The interference TNs are distributed as a PPP with density $\pi (D_0)^2$. Therefore, for TN i, the PDF of location (X, Y) is

$$f_{(X,Y)} = \frac{1}{\pi (D_0)^2}. \tag{10}$$

The CDF of distance $D_2^{(i)}$ can be calculated as

$$\begin{aligned} F_{D_2^{(i)}}(d_2^{(i)}) &= \iint\limits_{X^2+Y^2 \leq (d_2^{(i)})^2} \frac{1}{\pi (D_0)^2} \sqrt{X^2 + Y^2} dX dY \\ &\overset{(a)}{=} \int_0^{d_2^{(i)}} \int_0^{2\pi} \frac{r}{\pi (D_0)^2} d\theta dr \\ &= \left(\frac{d_2^{(i)}}{D_0} \right)^2 \end{aligned} \tag{11}$$

where (a) is obtained by using the following replacement:

$$\begin{cases} X = r\cos\theta \\ Y = r\sin\theta. \end{cases} \tag{12}$$

[3]Note that the approximation will be removed when the area of the considered is infinite.

Hence, based on (11), the PDF of $D_2^{(i)}$ is

$$f_{D_2^{(i)}}(d_2^{(i)}) = F'_{D_2^{(i)}}(d_2^{(i)}) = \frac{2d_2^{(i)}}{(D_0)^2}. \quad (13)$$

■

From Proposition 2, we can express the PDF of interference I_i generated by TN i as

$$f_{I_i}\left(I_i = Pg(d_2^{(i)})\right) = f_{D_2^{(i)}}(d_2^{(i)}) = \frac{2d_2^{(i)}}{(D_0)^2}. \quad (14)$$

The total interference, denoted by $I(N_I, \mathbf{D}_2)$, is related to the number of interference TNs N_I and the distance $\mathbf{D}_2$ of these interference TNs. From (7) and (13), we have the PDF of $I(N_I, \mathbf{D}_2)$

$$\begin{aligned} f_I(N_I = n_I, \mathbf{D}_2 = \mathbf{d}_2) &= f_{N_I}(n_I)\Pr(\mathbf{D}_2 = \mathbf{d}_2 | N_I = n_I) \\ &= f_{N_I}(n_I)\left(\frac{2}{(D_0)^2}\right)^{n_I} \prod_{n=1}^{n_I} d_2^{(n)}. \end{aligned} \quad (15)$$

As SINR expressed in (2) is related to D_1, N_I, and $\mathbf{D}_2$, the PDF of SINR can be expressed as

$$\begin{aligned} &f_{\mathrm{SINR}}(D_1 = d_1, N_I = n_I, \mathbf{D}_2 = \mathbf{d}_2) \\ &\quad = f_{D_1}(D_1 = d_1) f_I(N_I = n_I, \mathbf{D}_2 = \mathbf{d}_2) \end{aligned} \quad (16)$$

where f_{D_1} and f_I are given in (7) and (15), respectively.

B. TDP Transmission Successful Rate

When the received SINR is greater than the threshold β, a blockchain transaction transmission is successful. Therefore, we need to calculate the probability $\Pr(\mathrm{SINR} > \beta)$ which can be expressed as

$$\Pr(\mathrm{SINR} > \beta) = \iiint_{\Omega} f_{\mathrm{SINR}} d\Omega \quad (17)$$

where Ω is the area of $(D_1, N_I, \mathbf{D}_2)$ that satisfies $\mathrm{SINR}(D_1, N_I, \mathbf{D}_2) > \beta$. As f_{SINR} is obtained in (16), we only need to find the satisfied area Ω.

For the distance D_1 between the desired TN and the serving FN, it is safe to say that the SINR cannot be greater than β when $D_1 > D_0$. Thus, the satisfied range of D_1 is $[0, D_0]$. Then, for a given $D_1 = d_1$, we need to determine the satisfied number of interference TNs N_I as well as the locations of these TNs $\mathbf{D}_2$. To obtain the close-form expression of $\Pr(\mathrm{SINR} > \beta)$, we use the following approximation:

$$\text{the number of interference TNs } N_I \cong E(N_I) \quad (18)$$

where $E(N_I)$ is the expectation of random variable N_I. As the total number of TNs N_0 in IoT networks is usually quite large, this approximation is very accurate. In addition, it will be verified in the simulation in Section V that the approximation is very effective in all considered scenarios. Based on the TN distribution and transaction arrival models, we have

$$\begin{aligned} E(N_I) &= E(K) \cdot \Pr(\text{active}) \\ &= \pi (D_0)^2 \lambda_d (1 - \exp\{-2t\lambda_a\}) \\ &\triangleq \bar{n}_I \end{aligned} \quad (19)$$

where $\Pr(\text{active})$ is defined as (5). Thus, SINR is only related to D_1 and $\mathbf{D}_2$, and it can be rewritten as

$$\mathrm{SINR}(D_1, \mathbf{D}_2) = \frac{Pg(d_1)}{\sum_{i=1}^{\bar{n}_I} I_i + \sigma}. \quad (20)$$

For a given $D_1 = d_1$, we have

$$\begin{aligned} &\Pr(\mathrm{SINR}(D_1 = d_1, \mathbf{D}_2) > \beta) \\ &\quad = \Pr\left(\sum_{i=1}^{\bar{n}_I} I_i < \frac{Pg(d_1) - \sigma}{\beta}\right). \end{aligned} \quad (21)$$

Due to the high TN density in blockchain networks and the large radius of interference area D_0, $\bar{n}_I$ is a large number. Moreover, $I_i (i = 1, 2, \ldots, \bar{n}_I)$ is a set of random variables with independent identically distribution, and thus $\sum_{i=1}^{n_I} I_i$ can be seen as a normal distribution $N(\mu_I, {\delta_I}^2)$, where $\mu_I = \bar{n}_I E(I_i)$ and $\delta_I = \sqrt{\bar{n}_I} D(I_i)$ [26]. Note that $E(I_i)$ and $D(I_i)$ is the expectation and variance of variable I_i, respectively. In the following, we give the derivations of μ_I and δ_I, respectively:

$$\begin{aligned} \mu_I &= \bar{n}_I E(I_i) \\ &= \bar{n}_I \int_{d_2^{(i)} = d_{\min}}^{D_0} Pg(d_2^{(i)}) \Pr(D_2^{(i)} = d_2^{(i)}) d(d_2^{(i)}) \\ &= \bar{n}_I \int_{d_2^{(i)} = d_{\min}}^{D_0} Pg(d_2^{(i)}) \frac{2d_2^{(i)}}{(D_0)^2} d(d_2^{(i)}) \\ &= \frac{2P\bar{n}_I}{(D_0)^2}\left(d_2^{(i)}[G(D_0) - G(d_{\min})] - \bar{G}(D_0) - \bar{G}(d_{\min})\right) \end{aligned} \quad (22)$$

where G is the primitive function of path loss model $g(d)$, and $\bar{G}$ is the primitive function of G

$$\begin{aligned} \delta_I &= \sqrt{\bar{n}_I} D(I_i) \\ &= \sqrt{\bar{n}_I}\left(E\left({I_i}^2\right) - E^2(I_i)\right) \\ &= \sqrt{\bar{n}_I}\left[\int_{d_2^{(i)} = d_{\min}}^{D_0} P^2 g^2\left(d_2^{(i)}\right) \frac{d_2^{(i)}}{2(D_0)^2} d\left(d_2^{(i)}\right) - \left(\frac{\mu_I}{\bar{n}_I}\right)^2\right]. \end{aligned} \quad (23)$$

Denote $I = \sum_{i=1}^{\bar{n}_I} I_i$, and $I \sim N(\mu_I, {\delta_I}^2)$. Let $Y = ([I - \mu_I]/\delta_I)$, and thus $Y \sim N(0, 1)$. Therefore,

$$\begin{aligned} \Pr\left(\sum_{i=1}^{\bar{n}_I} I_i < \frac{Pg(d_1) - \sigma}{\beta}\right) &= \Pr\left(Y < \frac{\frac{Pg(d_1) - \sigma}{\beta} - \mu_I}{\delta_I}\right) \\ &= \Phi(\xi(d_1)) \end{aligned} \quad (24)$$

where

$$\xi(d_1) = \left[\frac{Pg(d_1) - \sigma}{\beta} - \mu_I\right] \Big/ \delta_I$$

Φ is the cumulative density function of standard normal distribution. Therefore, we have

$$\begin{aligned} \Pr(SINR > \beta) &= \iiint_{\Omega} f_{\mathrm{SINR}} d\Omega \\ &= \int_{d_1 = d_{\min}}^{D_0} f_{D_1}(d_1) \Phi(\xi(d_1)) d(d_1). \end{aligned} \quad (25)$$

Note that (25) is actually the close-form expression of $\Pr(\mathrm{SINR} > \beta)$ which can be calculated analytically when function f_{D_1}, the value of μ_I and δ_I as well as the parameters β and σ are given.

C. Overall Communication Throughput

Denote by R the overall required communication throughput, which can be expressed as

$$R = L\Pr(\text{SINR} > \beta)\left(\sum_{i=1}^{N_0} M_i\right),\ 0 \le R \le W \tag{26}$$

where N_0 is the total number of TNs, M_i is the number of arrived transactions for TN i, and W is the communication throughput when the transaction throughput reaches to the maximum value. For the given λ_d and λ_f, N_0, L, and $\Pr(\text{SINR} > \beta)$ are constant, while M_i is a set of independent identically PPP distributed random variables with parameter $\lambda_a T$. Let $M = \sum_{i=1}^{N_0} M_i$. As N_0 is a large number, M is a random variable with normal distribution $N(\mu_M, {\delta_M}^2)$, where $\mu_M = N_0 E(M_i)$ and $\delta_M = \sqrt{N_0} D(M_i)$ [26]. As M_i is distributed as a PPP, $E(M_i) = \lambda_a T$, and $D(M_i) = \lambda_a T$. Therefore, we have

$$\mu_M = N_0 \lambda_a T \tag{27}$$

$$\delta_M = \sqrt{N_0}\lambda_a T. \tag{28}$$

As mentioned in Section II, the maximum required communication throughput by the blockchain system in time T is W. Considering this constraint, Proposition 3 gives the PDF of R.

Proposition 3: For the given λ_d and λ_f, the PDF of overall required communication throughput R is

$$f_R(r = mL\Pr(\text{SINR} > \beta)) = \begin{cases} f_M(m) = N\left(\mu_M, {\delta_M}^2\right), & r < W \\ 1 - \Phi(m^*), & r = W \end{cases} \tag{29}$$

where Φ is the cumulative density function of standard normal distribution, and

$$m^* = \frac{\frac{W}{L\Pr(\text{SINR}>\beta)} - \mu_M}{\delta_M}. \tag{30}$$

Proof: For the given λ_d and λ_f, L and $\Pr(\text{SINR} > \beta)$ are constant. If the overall communication throughput $r < W$, we have $f_R(r) = f_M(m) = N(\mu_M, {\delta_M}^2)$. If $r = W$, $mL\Pr(\text{SINR} > \beta) = W$, and thus $m = (W/[L\Pr(\text{SINR} > \beta)]) \triangleq \widetilde{m}$. Due to the maximum transaction throughput (MTT) constraint, we have $f_R(r = W) = \Pr(M \ge \widetilde{m})$. Let $Y = ([M - \mu_M]/\delta_M)$, and thus $Y \sim N(0, 1)$ as $M \sim N(\mu_M, {\delta_M}^2)$. Thus, $\Pr(M \ge \widetilde{m}) = \Pr(Y \ge [(\widetilde{m} - \mu_M)/\delta_M]) = 1 - \Phi([(\widetilde{m} - \mu_M)/\delta_M])$, where Φ is the cumulative density function of standard normal distribution. ∎

IV. Optimal FN Deployment

For a given TN deployment, we can increase communication throughput by deploying more FNs, and thus support higher blockchain transaction throughput. However, as mentioned in Section II-A, once the transaction throughput reaches the maximum value, increasing communication throughput cannot improve the transaction throughput any more. Thus, for the sake of saving cost, it is worth to minimize the FN density subject to the blockchain transaction throughput constraint.

From (26), we know that R is a function of both λ_f and M, given λ_d and λ_a. To explore the relationship between FN density λ_f and TN density λ_d, we use $E(M) = \mu_M$ to calculate the conditional expectation of R as

$$\ddot{E}(R) = E\left(R \middle| M = \mu_M\right) = \min\{L\Pr(\text{SINR} > \beta)\mu_M, W\}. \tag{31}$$

Equation (31) shows that the overall communication throughput should increase with the number of transactions at the start, and stay unchanged when it reaches the maximum value W (i.e., the blockchain transactions saturated). According to (31), we find that $\ddot{E}(R)$ can exactly depict this relationship. Therefore, the following Definition 1 states the optimal FN deployment.

Definition 1: For given λ_d and λ_a, the FN deployment Θ is optimal if the Poisson distribution density $\lambda_f{}^*$ satisfies $\lambda_f{}^* = \arg\min_{\lambda_f}(\ddot{E}(R) = W)$.

According to Definition 1, the optimal FN deployment problem can be formulated as

$$\begin{aligned} \min\quad & \lambda_f \\ \text{s.t.}\quad & \ddot{E}(R) = W. \end{aligned} \tag{32}$$

Due to the complexity of $\Pr(\text{SINR} > \beta)$, we cannot find the optimal $\lambda_f{}^*$ in a close-form solution. Fortunately, as the monotonous increase for $\Pr(\text{SINR} > \beta)$ with FN density λ_f, we design Algorithm 1 to find the optimal value of FN density $\lambda_f{}^*$ for a given λ_d and λ_a. In Algorithm 1, we first calculate the value of $\bar{n}_I$, μ_I, δ_I, and $\xi(d_1)$, and then determine the searching region of FN density, finally, we find the optimal FN density in the searching region. The detailed steps are stated in Algorithm 1.

Algorithm 1 Algorithm of Optimal FN Deployment

Input: all the parameters (except λ_f) and the termination parameter $\epsilon > 0$.

Output: optimal FN density $\lambda_f{}^*$.

Initialization:

1: calculate $\bar{n}_I$, μ_I, δ_I and $\xi(d_1)$.

Find searching region:

2: set $\lambda_f{}^0$ as the initial value
3: calculate $\Pr(SINR > \beta)$ and $\ddot{E}(R)$ based on $\lambda_f{}^0$
4: **if** $\ddot{E}(R) < W$ **then**
5: $\lambda_f{}^0 = 2\lambda_f{}^0$ and go back to line 3
6: **else**
7: break
8: **end if**

Search stage:

9: set $a = \frac{\lambda_f{}^0}{2}$, $b = \lambda_f{}^0$
10: **while** $|b - a| > \epsilon$ **do**
11: set $\lambda_f{}^* = \frac{a+b}{2}$
12: calculate $\Pr(SINR > \beta)$ and $\ddot{E}(R)$ based on $\lambda_f{}^*$
13: **if** $\ddot{E}(R) < W$ **then**
14: set $a = \lambda_f{}^*$
15: **else**
16: set $b = \lambda_f{}^*$
17: **end if**
18: **end while**
19: **output** $\lambda_f{}^*$

We find that the major computational complexity of our optimal FN deployment Algorithm 1 lies on the search stage, where we should determine the optimal FN density from the range $[({\lambda_f}^0/2), {\lambda_f}^0]$. In the worst case, we need search $\log_2 \lceil {\lambda_f}^0/2\epsilon \rceil$ rounds, where ϵ is the termination parameter. In each round, we should calculate $\ddot{E}(R)$, and compare it with the maximum value W, thus determine the new search area for the next round. The computational complexity of these operations in a round can be seen as a constant, denoted as $O(1)$. Therefore, the total computational complexity of Algorithm 1 is $O(\log_2 \lceil {\lambda_f}^0/2\epsilon \rceil)$.

V. Security Performance Analysis

In this section, we analyze the security performance in the proposed system. Specifically, our analysis focuses on three typical attacks: 1) eclipse attack; 2) random link attack; and 3) random FN attack.

A. Eclipse Attack

As stated in [27], eclipse attack is defined as that the attacker monopolizes all the downlink and uplink connections of a TN (denoted as a victim), thus isolating the victim from the rest of the network. The attacker in this way can filter the victim's view of the blockchain, and conduct some activities for his own purposes, such as disrupting the blockchain network, wasting the computer power, etc. [27]. To make eclipse attacks more difficult, several countermeasures have been proposed in [27], including deterministic random eviction, random selection, test before evict, etc.

Besides these countermeasures in [27], we can also exploit wireless channel characteristics as well as blockchain protocols to further address eclipse attacks. Eclipse attacks can be addressed from two aspects: 1) physical layer security aiming at protecting wireless links from attacks and 2) blockchain network protocols to avoid information modifications. Let us elaborate them, respectively.

Physical (PHY) layer security can be used to avoid the wireless links being attacked, and thus to address DoS problem. PHY-layer authentication techniques exploit the spatial decorrelation property of the PHY-layer information, such as received signal strength indicators, received signal strength, channel phase response, channel impulse responses, and channel state information to distinguish radio transmitters, and thus detect spoofing attacks with low overhead [28].

From blockchain network protocol perspective, private key technology should be used to avoid transaction information modifications. Private key is actually a string of characters, which is only known by TN itself. Each TN owns a pair of private key and public key. The private key is used to sign the transactions [22]. The transactions can only be made with private and public keys. Thus, even the links of the victim TN are monopolized the transaction information cannot be modified by the attacker due to the lack of private key.

Therefore, by using the technologies of physical layer security and blockchain network protocol (authentication encryption), eclipse attacks could be dealt with effectively. Moreover, as discussed in Section II-A, when the attacked TNs are uniformly distributed in the network, the proposed framework is still valid by reducing the TNs density accordingly. We will conduct a simulation to examine the system performance when this kind of attack exists in the network, which will be presented in Section VI.

B. Random Link Attack

Random link attack is stated as that some links are randomly attacked or blocked due to the unstable wireless channel. This can be improved by PHY-layer security technology as well. Besides PHY-layer security technology, the following method can be used for addressing this attack. By sending some acknowledgment signaling [e.g., hybrid automatic repeat request (HARQ) in LTE system], TNs can judge whether the current wireless link is blocked. If the link is blocked, the corresponding TN will connect to another nearby FN via a nonattacked wireless link. Due to the increase of the distance between the TN and its serving FN, the TDP transmission successful probability [i.e., $\Pr(\text{SINR} > \beta)$] will be decreased. This can be derived from (25). Therefore, the transaction throughput could be decreased with the same FN density. However, as all FNs have the whole blocks, thus the transaction security can also be guaranteed in this case. Similar to eclipse attack, simulation results will be presented in Section VI to show the validity of our model in the presence of this attack.

C. Random FN Attack

Random FN attack is defined as that the attacker randomly monopolizes some FNs, thus the FNs cannot communicate with any TNs in this case. For a specific attacked FN, it cannot serve any TNs. Based on Proposition 1, Proposition 2 and (25), we know that the system performance in terms of SINR, TDP transmission successful rate, transaction throughput, etc., could be degraded. However, similar to the above two cases, when the FN are uniformly/randomly attacked, the framework proposed by this paper is valid by reducing the FNs density accordingly. We also conduct some simulation experiments to verify this, which will be presented in Section VI.

VI. Numerical Results and Discussion

In this section, we first validate the accuracy of our theoretical analysis by comparing the theoretical results with the simulation results in different typical scenarios. Then, we evaluate the relationship between blockchain transaction throughput and wireless communication throughput and demonstrate how the latter can cause a bottleneck for the former. Next, we give the optimal FN deployment under different TN densities. Finally, we evaluate the performance of the proposed system with three typical attacks.

A. Simulation Settings

We consider an IoT network that is composed of multiple TNs operating blockchain transactions and multiple FNs supporting blockchain service. The network coverage is set as a circular area with radius 150 m. The radius of interference area is $D_0 = 50$ m. The transmit power of TN is 20 dBm, and the noise power is -104 dBm [29]. The transaction packet length is 256 bits [30], and the transaction arrival rate is

TABLE II
SIMULATION PARAMETERS

Parameter	Value
The radius of considered area	150 m
The radius of interference area D_0	50 m
TN transmit power P	20 dBm
Path loss model $g(d)$	$g(d) = d^{-2.5}$ [17]
Total time T	10000 s
Transaction packet length L	256 bits [30]
Transaction arrival density λ_a	$\frac{1}{1800} s^{-1}$ [24]
Noise power σ	-104 dBm [29]

$(1/1800)$ s^{-1} [24]. The total considered time is 10 000 s. For convenience, all the parameters are summarized as Table II.

B. Performance Evaluations Without Attacks

In the first experiment, we examine the TDP transmission successful rate, i.e., the probability Pr(SINR $> \beta$), with fixed FN density 320 per km^2 and varying TN density. The analytical results are computed from (25). In detail, we first calculate f_{D_1} (the PDF of D_1) based on Proposition 1. We then obtain the value of μ_I and δ_I by using (22) and (23), respectively, and thus the value of $\xi(d_1)$. Substituting them in (25), we get Pr(SINR $> \beta$). For simulations, if the received SINR for a transaction transmission is greater than β, this transaction is transmitted successfully, otherwise it counts as a failure. Fig. 4 shows the probability Pr(SINR $> \beta$) for both analytical and simulation results with different TN densities under SINR threshold parameter $\beta = -15$ dB and $\beta = -9$ dB. From this figure, we can see that the curves of analytical results for both β match closely to those of simulations. For example, the successful rate for analytical results and simulations is 76% and 77%, respectively, when the TN density equals to 1.0×10^5 and $\beta = -15$ dB, implying that the difference between the analytical results and simulations is trivial. Moreover, as expected, under both $\beta = -15$ dB and $\beta = -9$ dB scenarios the probability Pr(SINR $> \beta$) decreases with the TN density due to the increasing interference. We also find that Pr(SINR $> \beta$) is much lower under $\beta = -9$ dB than that under $\beta = -15$ dB with the same TN density due to the stringent SINR requirement.

In the second experiment, we compare the TDP transmission successful rate with fixed TN density 1.0×10^5 per km^2 but varying FN densities. The analytical and simulation results are both obtained in the same way as stated in the first experiment. Fig. 5 shows the probability Pr(SINR $> \beta$) for both analytical and simulation results with different FN densities under SINR threshold parameter β. From this figure, we again find that the differences between the analytical and simulation results are always very small (for example, 4% for $\beta = -15$ dB and 3% for $\beta = -9$ dB when FN density is 200 per km^2). These numerical results clearly validate the accuracy of the our modeling and show the effectiveness of the approximation in (19). Moreover, Pr(SINR $> \beta$) increases with the FN density due to the decreasing distance between the desired TN and the serving FN.

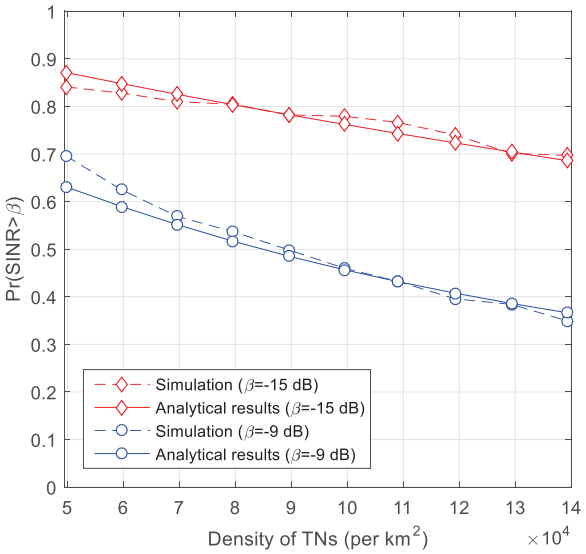


Fig. 4. Comparisons of Pr(SINR $> \beta$) versus TN density (FN density is per 320 km^2).

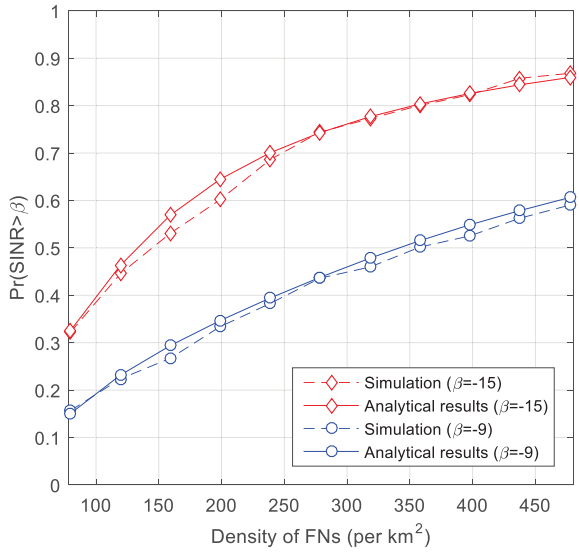


Fig. 5. Comparisons of Pr(SINR $> \beta$) versus FN density (TN density is 1.0×10^5 per km^2).

Next, we evaluate the performance of overall communication throughput as a function of TN density. Considering the characteristics of the new block generation in blockchain system (e.g., a new block with size 1 MB transaction data is generated every 10 min in Bitcoin [15]), the overall communication throughput in this paper is calculated as follows: the total data volume that is successfully transmitted in every 10 min for all TNs. Due to the limitation of the MTT in blockchain, the overall required communication throughput will stay unchanged once the transaction throughput achieves the MTT. Fig. 6 shows the overall throughput with varying TN density from 1.0×10^5 to 1.0×10^6 per km^2 under different parameters β and MTT. The FN density is fixed to 5000 per km^2. From Fig. 6, we can see that the communication throughput for all the four scenarios is increased when the TN density is low. With TN density increasing,

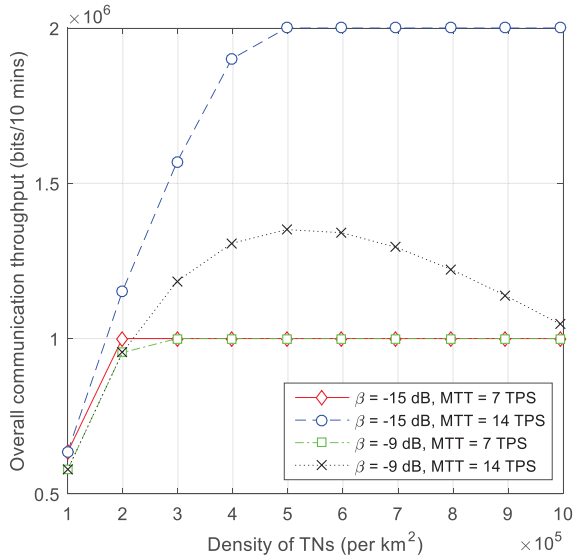


Fig. 6. Comparisons of overall throughput versus TN density (FN density is 5000 per km^2).

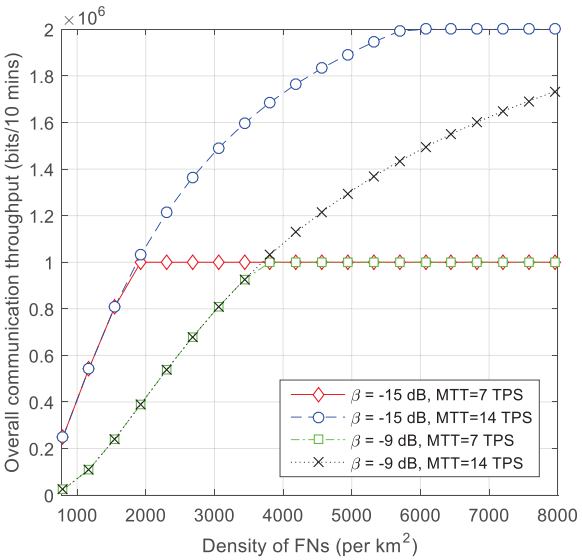


Fig. 7. Comparisons of overall throughput versus FN density (TN density is 40 000 per km^2).

the curve with parameters $\beta = -15$ dB, MTT $=$ 7TPS, $\beta = -9$ dB, MTT $=$ 7TPS, and $\beta = -15$ dB, MTT $=$ 14TPS arrives to the maximum communication throughput sequentially. The curve with parameters $\beta = -9$ dB, MTT $=$ 14TPS cannot achieve the maximum throughput under any TN density scenario. Note that the throughput is not the maximum value when TN density is 5×10^5 per km^2, as it does not stay unchanged after that. When the TN density is greater than 5×10^5 per km^2, the overall communication throughput for the parameter pair $\beta = -9$ dB, MTT $=$ 14TPS is decreased due to the high interference. This provides a valid theoretical guidance for the blockchain-enabled IoT system design.

In the next experiment, we investigate the relationship between the overall communication throughput and FN density with fixed TN density 4.0×10^5 per km^2. Intuitively, under a given TN density, the more FNs are deployed, the

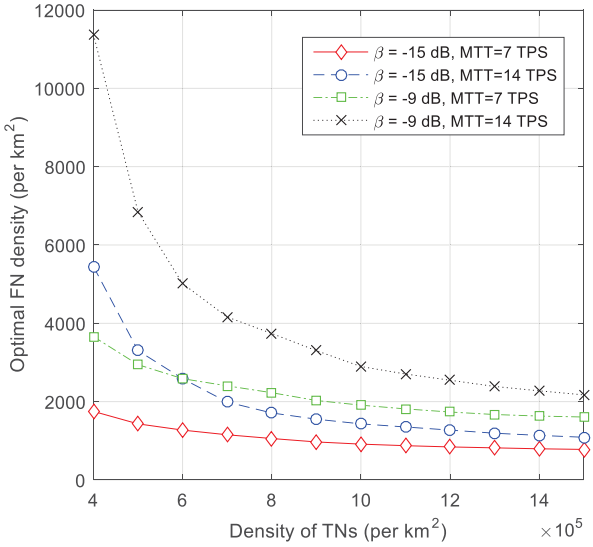


Fig. 8. Comparisons of optimal FN density versus TN density.

greater SINR would be received, and thus the higher overall communication throughput can be achieved. Fig. 7 shows the overall communication throughput with varying FN density from 1000 to 8000 per km^2 under different parameters β and MTT. From this figure, we can see that the communication throughput for all the four scenarios is increased when the FN density is low. When the throughout reaches the maximum value, it is unchanged which means that the transaction throughput achieves the MTT. For example, under the circumstance $\beta = -15$ dB, MTT $=$ 7TPS, when the FN density is higher than around 2000 per km^2, the communication throughput is unchanged, which means that under the TN density 4.0×10^5 per km^2 the optimal FN density is about 2000 per km^2. Similarly, we can find that the optimal FN density with fixed TN density 4.0×10^5 per km^2 for $\beta = -9$ dB, MTT $=$ 7TPS, $\beta = -15$ dB, MTT $=$ 14TPS, and $\beta = -9$ dB, MTT $=$ 14TPS is about 4000 per km^2, 5800 per km^2, and larger than 8000 per km^2, respectively.

Next, we investigate the optimal FN deployment with different TN densities. Fig. 8 shows the optimal FN density with varying TN density from 4.0×10^5 to 1.5×10^6 per km^2 under different parameters β and MTT. From this figure, we can find that when the TN density is lower than 8.0×10^5 per km^2, the optimal FN density decreases rapidly. The rationale behind is that the more TNs are deployed, the more transactions happen in time T, the easier to achieve the maximum throughput, and thus the less number of FNs are needed. However, when the TN density is higher than 8.0×10^5 per km^2, the optimal FN density is changed slowly. This is because that the high interference is introduced resulting in low TDP transmission successful rate. Therefore, although the number of transactions is increased, the overall throughput is changed slowly, and thus the change of the optimal FN density is also slow.

C. Performance Evaluations With Attacks

In the following, we conduct experiments to examine our system performance in term of overall communication throughput for the three typical attacks, eclipse attack, random link attack, and random FN attack. All the three kinds of

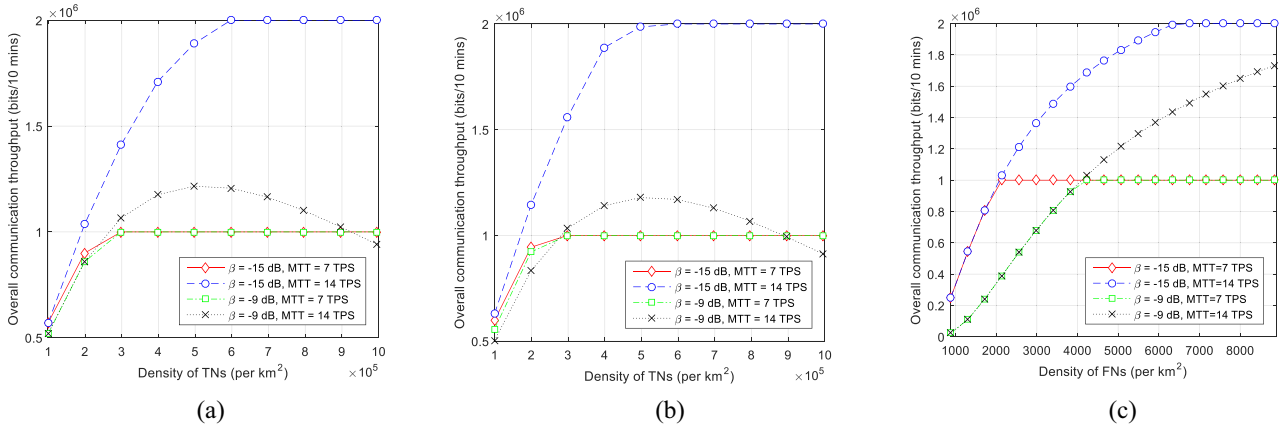


Fig. 9. Comparisons of overall throughput with three typical kind of attacks. (a) Eclipse attacks (FN density is 5000 per km^2). (b) Random link attacks (FN density is 5000 per km^2). (c) Random TN attacks (TN density is 40 000 per km^2).

attacks are set to be distributed uniformly with 10% percentage, while the other parameters remain the same as Table II. Fig. 9 shows the comparisons of overall throughput with three kinds of attacks in the system. From all the three subfigures, we find that the trend of the four curves remain the same as Figs. 6 and 7, while the absolute value of overall communication throughput for all four curves reduces due to the attacks. Specifically, in Fig. 9(a) the overall communication throughput is reduced about 10% compared with that in Fig. 6. This is because that once a TN is suffered from eclipse attacks, it cannot contribute any communication throughput as all links are monopolized. In Fig. 9(b), we find that the degradation of overall communication throughput is much smaller than 10% compared with that in Fig. 6. This is because that the attacker cannot control all the connections for a TN in this case, thus the TN can still contribute some communication throughput although the wireless channel condition may be degraded. As expected, the degradation of overall communication throughput in Fig. 9(c) is about 10% compared with that in Fig. 7 due to the attacked FNs. These results also demonstrate that our analysis framework can still validate in the systems with attacks.

VII. Conclusion

In this paper, we investigated the performance of blockchain-enabled IoT networks. We first theoretically analyzed SINR, TDP transmission successful rate as well as overall communication throughput by considering the characteristics of blockchain in spatio-temporal domain. Then, based on the performance analysis, we designed an optimal blockchain full FN deployment scheme to achieve the maximum transaction and communication throughput with the minimum full FN density. Finally, we analyzed the security performance in the system with three typical kinds of attacks, where we have proposed to adopt approaches such as physical layer security algorithms to mitigate these attacks. Numerical results validated the accuracy of our theoretical analysis, and the difference between simulation and analytical results is usually less than 4%.

The work in this paper provides a framework for the blockchain-enabled wireless IoT system design through a detailed spatio-temporal model. It can be served as a foundation for future research on system performance analysis, protocols, and algorithms design. For instance, one potential research topic is to use this model to develop new and optimized communication protocols by considering the broadcasting natural in blockchain systems. In addition, by adopting physical layer security techniques, secure wireless blockchain system design against active attacks can be a promising research topic.

References

[1] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Bus. Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[2] A. Bassi and G. Horn, "Internet of Things in 2020: A roadmap for the future," *Eur. Commission Inf. Soc. Media*, vol. 22, pp. 97–114, Aug. 2008.

[3] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 1–6, 2015.

[4] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design*, San Jose, CA, USA, 2014, pp. 417–423.

[5] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[6] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–275, 2018.

[7] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ, USA: Princeton Univ. Press, 2016.

[8] M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Bus. Rev.*, vol. 95, no. 1, pp. 118–127, 2017.

[9] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[10] Group BitFury. (Sep. 2015). *Proof of Stake Versus Proof of Work*. Accessed: Sep. 28, 2018. [Online]. Available: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf

[11] S. Popov. (Apr. 2018). *The Tangle*. Accessed: Sep. 28, 2018. [Online]. Available: https://www.iota.org/research/academic-papers

[12] *Blockchain and the Internet of Things: The IoT Blockchain Opportunity and Challenge*. Accessed: Sep. 21, 2018. [Online]. Available: https://www.i-scoop.eu/blockchain-distributed-ledger-technology/blockchain-iot/

[13] C. MacGillivray *et al.*, "IDC future scape: Worldwide Internet of Things 2017 predictions," in *Proc. IDC Web Conf.*, 2016.

[14] A. Dorri, S. S. Kanhere, and R. Jurdak. (2016). *Blockchain in Internet of Things: Challenges and Solutions*. [Online]. Available: http://arXiv preprint arXiv:1608.05187

[15] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. USENIX Symp. Netw. Syst. Design Implement.*, 2016, pp. 45–59. [Online]. Available: http://arxiv.org/abs/1510.02037

[16] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.
[17] K. Smiljkovikj, P. Popovski, and L. Gavrilovska, "Analysis of the decoupled access for downlink and uplink in wireless heterogeneous networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 2, pp. 173–176, Apr. 2015.
[18] T. Bai and R. W. Heath, "Coverage and rate analysis for millimeter-wave cellular networks," *IEEE Trans. Commun.*, vol. 14, no. 2, pp. 1100–1114, Feb. 2015.
[19] Y. Zhong, T. Q. S. Quek, and X. Ge, "Heterogeneous cellular networks with spatio-temporal traffic: Delay analysis and scheduling," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1373–1386, Jun. 2017.
[20] N. Sapountzis, T. Spyropoulos, N. Nikaein, and U. Salim, "An analytical framework for optimal downlink-uplink user association in HetNets with traffic differentiation," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, 2015, pp. 1–7.
[21] Y. Zhong, G. Wang, R. Li, and T. Q. S. Quek. (2018). *Effect of Spatial and Temporal Traffic Statistics on the Performance of Wireless Networks*. [Online]. Available: http://arXiv preprint arXiv:1804.06754
[22] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
[23] T. Huimin, S. Yong, and D. Peiwu, "Public blockchain evaluation using entropy and TOPSIS," *Expert Syst. Appl.*, vol. 117, pp. 204–210, May 2018.
[24] "Cellular system support for ultra low complexity and low throughput Internet of Things (CIoT), v13.10," 3GPP, Sophia Antipolis, France, Rep. TR 45.820, 2015.
[25] *LTE Physical Layer—General Description, Release 8*, 3GPP Standard TS 36.201, 2007.
[26] P. L. Hsu and H. Robbins, "Complete convergence and the law of large numbers" *Proc. Nat. Acad. Sci. USA*, vol. 33, no. 2, pp. 25–31, 1947.
[27] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in *Proc. USENIX Security Symp.*, 2015, pp. 129–144.
[28] L. Xiao, X. Wan, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced overhead," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1676–1687, Mar. 2018.
[29] Y. Sun, G. Feng, S. Qin, and S. Sun, "Cell association with user behavior awareness in heterogeneous cellular networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4589–4601, May 2018.
[30] S. Chen, J. Zhang, R. Shi, J. Yan, and Q. Ke, "A comparative testing on performance of blockchain and relational database: Foundation for applying smart technology into current business systems," in *Proc. Int. Conf. Distrib. Ambient Pervasive Interact.*, 2018, pp. 21–34. [Online]. Available: http://link.springer.com/10.1007/978-3-642-39351-8

Yao Sun received the B.S. degree in mathematical sciences from the University of Electronic Science and Technology of China, Chengdu, China, where he is currently pursuing the Ph.D. degree at the National Key Laboratory of Science and Technology on Communications.

His current research interests include blockchain system, Internet of Things, and resource management in mobile networks.

Lei Zhang (SM'18) received the Ph.D. degree from the University of Sheffield, Sheffield, U.K.

He was a Research Engineer with the Huawei Communication Technology Laboratory, Shenzhen, China, and a Research Fellow with 5G Innovation Centre (5GIC), Institute of Communications, University of Surrey, Guildford, U.K. He is currently a Lecturer with the University of Glasgow, Glasgow, U.K. He holds 16 U.S./U.K./EU/China granted patents on wireless communications and also holds a visiting position with 5GIC, University of Surrey. His current research interests include communications and array signal processing, including radio access network slicing, wireless blockchain systems, new air interface design, Internet of Things, multiantenna signal processing, massive MIMO systems, and full-duplex.

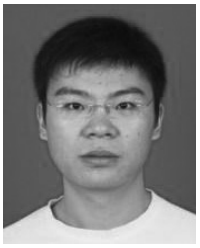
Dr. Zhang is an Associate Editor of IEEE ACCESS.

Gang Feng (M'01–SM'06) received the B.Eng. and M.Eng. degrees in electronic engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 1986 and 1989, respectively, and the Ph.D. degree in information engineering from the Chinese University of Hong Kong, Hong Kong, in 1998.

He joined the School of Electric and Electronic Engineering, Nanyang Technological University, Singapore, in 2000 as an Assistant Professor and became an Associate Professor in 2005. He is currently a Professor with the National Laboratory of Communications, University of Electronic Science and Technology of China. He has extensive research experience and has been published widely in computer networking and wireless networking research. His current research interests include resource management in wireless networks and next generation cellular networks.

Bowen Yang received the B.Sc. degree in optical information science and technologies from the North University of China, Taiyuan, China, in 2009, and the M.Sc. degree in communications and signal processing from the Newcastle University, Newcastle upon Tyne, U.K., in 2015. He is currently pursuing the Ph.D. degree at the School of Engineering, University of Glasgow, Glasgow, U.K.

His current research interests include wireless network slicing and Internet of Things as well as interference cancelation in wireless networks.



Bin Cao (A'17) received the B.S. degree in communications engineering from the Xi'an University of Technology, Xi'an, China, in 2006, the M.S. degree in communications and system information from the Chongqing University of Posts and Telecommunications, Chongqing, China, in 2010, and the Ph.D. degree (Hons.) in communication and information systems from the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu, China, in 2014.

He was an Associate Professor with the Chongqing University of Posts and Telecommunications. He is an Associate Professor with the Institute of Network Technology, Beijing University of Posts and Telecommunications, Beijing, China. In 2012, he was an International Visitor with the Institute for Infocomm Research, Singapore, for eight months. He was a Research Fellow with the National University of Singapore, Singapore, from 2015 to 2016. His current research interests include blockchain system, Internet of Things, and mobile edge computing.

Dr. Cao has served as the Symposium Co-Chair for IEEE ICNC 2018 and as a TPC member for numerous conferences.

Muhammad Ali Imran (M'03–SM'12) is a Professor of wireless communication systems with the University of Glasgow, Glasgow, U.K., where he is involved with research on self-organized networks, wireless networked control systems, and the wireless sensor systems, where he heads the Communications, Sensing and Imaging CSI Research Group. He is an Affiliate Professor with the University of Oklahoma, Norman, OK, USA, and a Visiting Professor with the 5G Innovation Centre, University of Surrey, Guildford, U.K. He has over 20 years of combined academic and industry experience with several leading roles in multimillion pounds funded projects. He has filed 15 patents. He has authored or co-authored over 400 journal and conference publications. He has edited 3 books and authored over 20 book chapters, and has successfully supervised over 40 postgraduate students at the doctoral level. He has been a Consultant to international projects and local companies in the area of self-organized networks.

Mr. Imran is a Fellow of the IET and a Senior Fellow of the HEA.