2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)

Performance Analysis for Blockchain Driven Wireless IoT Systems Based on Tempo-Spatial Model

Yao Sun*, Lei Zhang† *Senior Member, IEEE*, Gang Feng* *Senior Member, IEEE*,
Bowen Yang†, Bin Cao‡, Muhammad Ali Imran† *Senior Member, IEEE*
* National Key Lab. on Communications, University of Electronic Science and Technology of China, Chengdu, China
† School of Engineering, University of Glasgow, Glasgow
‡ Institute of Network Technology,
Beijing University of Posts and Telecommunications, Beijing, China
Email: sunyao@std.uestc.edu.cn, {lei.zhang, muhammad.imran}@glasgow.ac.uk, fenggang@uestc.edu.cn,
b.yang.1@research.gla.ac.uk, caobin65@163.com

***Abstract*—Blockchain has shown a great potential for Internet of Things (IoT) systems to establish trust and consensus mechanisms with no involvement of any third party. It has been not clear how the low complexity devices and the wireless communications among them can pose constraints on the blockchain enabled IoT systems. In this paper, we establish a fundamental analysis model to underpin the blockchain enabled IoT system. By considering spatio-temporal domain Poisson distribution, i.e., node geographical distribution 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. Then, based on the analytical model, we design an optimal full function node deployment for blockchain system to achieve the maximum transaction throughput with the minimum full function node density. Numerical results validate the accuracy of our theoretical analysis and evaluate the relationship between blockchain full function node deployment and the density of IoT nodes.**

I. Introduction

Internet of Things (IoT) is envisioned as one of most promising techniques to form a globally distributed network, where interactions happen among not only humans but also machines/devices (e.g., cars, monitors, smart wearable devices etc.) [1]. Nevertheless, IoT devices are easily to be attacked due to the easy accessibility and lack of unified, normative standard [2], [3]. In the meanwhile, because of the limited power and storage space, it is difficult to implement sophisticated security approaches in most of the IoT devices. Moreover, the involvement of the third party in current centralized IoT system results in expensive processing overhead and makes the smart contract (such as micro payment and information exchange) in IoT ecosystem unattractive.

Impressive works have been executed to find proper solutions against the aforementioned issues, where blockchain has been drawing grossing attentions [4], [5]. Blockchain is a kind of decentralized database which is formed by a continuously growing set of data blocks [6]. The blockchain based decentralized network with reliable consensus mechanisms [7], [8] enables the progress/cost effective as well as information highly safe transactions, which can address IoT's trust and security concerns directly [9]–[11].

Though good prospects can be expected, wireless communications is of the issues that may hinder the blockchain enabled IoT system. The imperfect channel quality may introduce throughput and delay constraints, which are not considered in the traditional blockchain systems that perfect communication is typically assumed. Hence, it is necessary to investigate how the wireless communications can affect the performance of the blockchain enabled IoT system. As a fundamental work, a framework of analytical system model is critical for the blockchain enabled IoT performance analysis and system design. One particularity in such a system is that in addition to the geographically random distribution of the nodes in the traditional IoT systems, event triggered blockchain should take the time domain randomness into consideration, which may make the system significantly complex.

The existing performance analyses that focus on traditional wireless networks cannot be directly applicable to blockchain-enabled IoT system. Work [12]–[14] exploits stochastic geometry in spatial domain to evaluate the network performance for traditional cellular networks [12], heterogeneous cellular networks [13] and millimeter wave networks [14], respectively. While work [15] simultaneously considers spatial and time domains with combination of queueing theory and stochastic geometry to evaluate delay performance. To the best of the authors' knowledge, there is no analytical model dedicated for blockchain-enabled wireless IoT systems which can underpin communication and blockchain systems optimization.

In this paper, we establish a comprehensive and analytical system model for blockchain enabled IoT system model, and propose an optimal blockchain full function node deployment

978-1-7281-2542-8/19/$31.00 ©2019 IEEE
DOI 10.1109/CyberC.2019.00066

scheme based on the analysis. Specifically, we first derive the probability density function (PDF) of the transmission signal-to-interference-plus-noise ratio (SINR) from light IoT nodes to full function nodes considering both time (blockchain transaction arrival rate) and spatial(nodes geographic distribution) domain Poisson point process (PPP) modeling. The transaction successful rate and overall communication throughput are analytically calculated based on the derived expressions. Then, a searching algorithm to find the optimal blockchain full function node deployment is proposed, given certain IoT node density and blockchain transaction throughput. Finally, the effectiveness of our derivations are verified by simulations, where the difference between analytical results and simulation results is as low as 2%.

In the following, we present the blockchain-enabled wireless IoT network model in Section II. In Section III, we theoretically analyze the system performance, and propose an optimal blockchain full function node deployment in Section IV. We present numerical results in Section V and conclude this paper in Section VI.

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

The blockchain-enabled IoT network model is shown in Fig. 1, which consists of three main elements: full function nodes (FNs), IoT transaction nodes (TNs) and the transactions (any valuable information transmission between TNs can be considered as transactions).

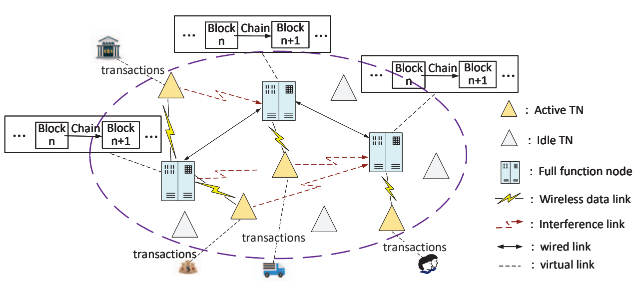

Fig. 1. Blockchain-enabled IoT network model

TNs are typically composed of low-end IoT devices. At any time point, each TN's status is either active (with data transmissions) or idle (with no data transmission). FNs are normally the authorized nodes with high computing and storage abilities. They have full functionalities with respect to blockchain protocols thus bare the responsibility for transaction confirmation, data storage and building new blocks. Once a new transaction arrives, the TN will broadcast the information to the whole network for verification, after which the FN who has the right of building a block will insert this transaction into the chain, and all FNs need to update their own database accordingly. Note that here we only focus on the uplink transmission analysis from TN to FN. The downlink analysis could be performed in a similar manner, which is omitted in this paper.

It is worth to clarify the difference of transaction throughput and communication throughput. Transaction throughput is the number of transactions that can be confirmed in a time unit by the blockchain system. Usually we use transactions per second (TPS) as the metric. Communication throughput is the amount of transmitted data in a time unit for this network. In the proposed system model, to achieve a certain level of transaction throughput C_T the communication throughput R need to satisfy

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

where L is the packet length for a transaction.

B. Wireless Communication Model

We present the wireless communication model of blockchain enabled IoT networks with respect to the spatio-temporal domain characteristics. First, in spatial domain, let $A \subseteq R^2$ be the considered area where TNs and FNs are assumed to be distributed as a homogeneous PPP with density λ_d and λ_f respectively. We assume that the minimum distance between TN and FN is d_{min}, and each TN is associated with the nearest FN. Then in time domain, we say a TN is in the active mode once a transaction is arrived. As the transaction packet length L is usually very short (e.g., 1KB in Bitcoin [16]), the transmission time (active time) t can be seen as a small constant with $t \ll T$, where T is the total considered time. Therefore, for a specific TN, ignoring the data transmission time t, the number of arrived transactions M in time T can be assumed to be a Poisson distribution with parameter $\lambda_a T$, where λ_a is the blockchain transaction arrival rate.

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

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

where D_1 is the distance between desired TN and the serving FN, $\mathbf{D}_2 = \left[D_2^{(1)}, D_2^{(2)}, ..., D_2^{(N_I)}\right]$ is the distance vector for all interference TNs, P is the transmit power of all TNs, N_I is the number of interference TNs, and σ is the noise power.

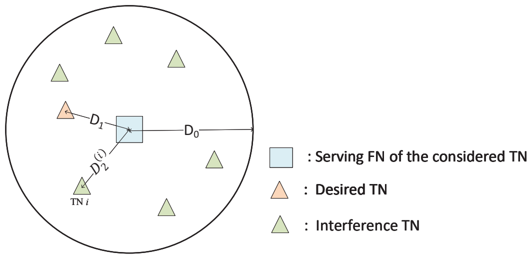

Fig. 2. Interference area for a specific TN

III. Wireless Performance Analysis in Blockchain-enabled IoT networks

In this section, we theoretically analyze the transmission performance in terms of uplink SINR as well as transaction data packet (TDP) transmission successful rate.

A. Probability Density Function of SINR

Let us start with SINR distribution analysis. As both TNs and FNs are assumed geographically distributed as homogeneous PPP, it is reasonable to investigate the SINR performance of any one arbitrary TN. For convenience, we use capital letters to denote random variables, and the corresponding lowercases to the value of random variables. The function f_X denotes the PDF of random variable X.

For a specific TN, the desired signal power S is a random variable that can be written as $S = Pg(D_1)$, where D_1 is the distance between TN and the serving FN. Considering the fact that $\Pr(D_1 > d_1) = \exp\{-\lambda_1 \pi (d_1)^2\}$, we have the PDF of D_1 as

$$f_{D_1}(d_1) = 2\pi\lambda_1 d_1 \exp\{-\lambda_1 \pi (d_1)^2\}. \tag{3}$$

Therefore, we obtain that the PDF of desired signal power as

$$f_S\big(S = Pg(d_1)\big) = f_{D_1}(d_1) = 2\pi\lambda_1 d_1 \exp\{-\lambda_1 \pi (d_1)^2\}. \tag{4}$$

We now study the distribution of the received interference. Based on Section II, the number of TNs K within the interference area is a 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 who 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

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

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 can be expressed as

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

Then we investigate the distance $D_2^{(i)}$ between an interference TN i and the FN. The cumulative distribution function (CDF) of distance $D_2^{(i)}$ can be calculated as

$$\begin{aligned} F_{D_2^{(i)}}(d_2^{(i)}) &= \iint\limits_{X^2+Y^2 \le (d_2^{(i)})^2} f_{(X,Y)} \sqrt{X^2+Y^2}\, dX dY \\ &= \iint\limits_{X^2+Y^2 \le (d_2^{(i)})^2} \frac{1}{\pi (D_0)^2} \sqrt{X^2+Y^2}\, dX dY \\ &= \left(\frac{d_2^{(i)}}{D_0}\right)^2 \end{aligned} \tag{8}$$

Hence, based on (8), the PDF of $D_2^{(i)}$ is

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

Therefore, the PDF of interference I_i generated by TN i is

$$f_{I_i}\big(I_i = Pg(d_2^{(i)})\big) = f_{D_2^{(i)}}(d_2^{(i)}) = \frac{2 d_2^{(i)}}{(D_0)^2}. \tag{10}$$

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 (9), we have the PDF of $I(N_I, \mathbf{D}_2)$

$$\begin{aligned} f_I(N_I = n_I, \mathbf{D}_2 = \mathbf{d}_2) &= f_{N_I}(n_I) \Pr(\mathbf{D}_2 = \mathbf{d}_2 | N_I = n_I) \\ &= f_{N_I}(n_I) \left(\frac{2}{D_0}\right)^k \prod_{n=1}^{k} (d_2)^n . \end{aligned} \tag{11}$$

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

$$\begin{aligned} & f_{SINR}(D_1 = d_1, N_I = n_I, \mathbf{D}_2 = \mathbf{d}_2) \\ & \quad = f_{D_1}(D_1 = d_1) f_I(N_I = n_I, \mathbf{D}_2 = \mathbf{d}_2), \end{aligned} \tag{12}$$

where f_{D_1} and f_I is expressed as (7) and (11), respectively.

B. TDP Transmission Successful Rate

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

$$\Pr(SINR > \beta) = \iiint\limits_{\Omega} f_{SINR}\, d\Omega, \tag{13}$$

where Ω is the area of D_1, N_I, $\mathbf{D}_2$ that satisfies $SINR(D_1, N_I, \mathbf{D}_2) > \beta$. As f_{SINR} is obtained in (12), we only need to find the satisfied area Ω.

For the distance D_1 between desired TN and the serving FN, we believe that the SINR cannot be greater than β when $D_1 > D_0$. Thus, the satisfied range of D_1 is $[0, D_0]$. As a result, 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 $\Pr(SINR > \beta)$, we use the following approximation,

$$\textit{The number of interference TNs } N_I \cong E(N_I), \tag{14}$$

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, and the effectiveness can also be verified by our simulations in Section V. Based on the TN distribution and transaction arrival models, we have

$$\begin{aligned} E(N_I) &= E(K) \cdot \Pr(active) \\ &= \pi \left(D_0\right)^2 \lambda_d (1 - \exp\{-2t\lambda_a\}) \triangleq \bar{n}_I, \end{aligned} \tag{15}$$

where $\Pr(active)$ is defined as (5). Under this approximation, SINR is only related to $D_1, \mathbf{D}_2$, and we have

$$\Pr\left(SINR\left(D_1 = d_1, \mathbf{D}_2\right) > \beta\right) = \Pr\left(\sum_{i=1}^{\bar{n}_I} I_i < \frac{Pg(d_1) - \sigma}{\beta}\right) \tag{16}$$

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, $I_i (i = 1, 2, \cdots, \bar{n}_I)$ 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 $\delta_I = \sqrt{\bar{n}_I} D(I_i)$ [17]. Note that $E(I_i)$ and $D(I_i)$ is the expectation and variance of variable I_i respectively. μ_I and δ_I can be easily calculated as follows when $g(d)$ is given.

$$\mu_I = \bar{n}_I E(I_i) = \bar{n}_I \int_{d_2^{(i)} = d_{min}}^{D_0} Pg(d_2^{(i)}) \Pr(D_2^{(i)} = d_2^{(i)}) d(d_2^{(i)}), \tag{17}$$

and

$$\delta_I = \sqrt{\bar{n}_I} D(I_i) = \sqrt{\bar{n}_I} \left(E\left({I_i}^2\right) - E^2\left(I_i\right)\right). \tag{18}$$

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

$$\begin{aligned} \Pr\left(\sum_{i=1}^{\bar{n}_I} I_i < \frac{Pg\left(d_1\right) - \sigma}{\beta}\right) &= \Pr\left(Y < \frac{\frac{Pg(d_1) - \sigma}{\beta} - \mu_I}{\delta_I}\right) \\ &= \Phi\left(\xi\left(d_1\right)\right). \end{aligned} \tag{19}$$

where $\xi\left(d_1\right) = \frac{\frac{Pg(d_1) - \sigma}{\beta} - \mu_I}{\delta_I}$, Φ is the cumulative density function of standard normal distribution. Therefore, we have

$$\Pr(SINR > \beta) = \int_{d_1 = d_{min}}^{D_0} f_{D_1}\left(d_1\right) \Phi\left(\xi\left(d_1\right)\right) d\left(d_1\right). \tag{20}$$

Note that (20) is actually the close-form expression of $\Pr(SINR > \beta)$ which can be calculate analytically when function f_{D_1}, the value of μ_I, δ_I as well as the parameters β, σ are given.

IV. Communication Throughput and Optimal Full Node Deployment

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

$$R = L \Pr\left(SINR > \beta\right) \left(\sum_{i=1}^{N_0} M_i\right), \ 0 \le R \le W \tag{21}$$

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 arrives to the maximum value. For the given λ_d and λ_f, N_0, L and $\Pr(SINR > \beta)$ are constants, 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 $\mu_M = N_0 E\left(M_i\right)$ and $\delta_M = \sqrt{N_0} D\left(M_i\right)$ [17]. As M_i is distributed as a PPP, $E\left(M_i\right) = \lambda_a T$, and $D\left(M_i\right) = \lambda_a T$. Therefore, we have

$$\mu_M = N_0 \lambda_a T, \tag{22}$$

$$\delta_M = \sqrt{N_0} \lambda_a T. \tag{23}$$

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

$$\begin{aligned} & f_R\left(r = mLPr\left(SINR > \beta\right)\right) \\ & \quad = \begin{cases} f_M\left(m\right) = N\left(\mu_M, {\delta_M}^2\right), & r < W \\ 1 - \Phi(\frac{\widetilde{m} - \mu_M}{\delta_M}), & r = W \end{cases}. \end{aligned} \tag{24}$$

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 achieves the maximum value, increasing communication throughput cannot improve the transaction throughput. Thus, an optimal FN deployment should support the maximum transaction throughput (also the maximum required communication throughput W as well) by using the minimum number of FNs. In the following, we will develop an algorithm to find the optimal FN deployment.

Given the parameters λ_d and λ_a, we define

$$E(R) = L\Pr\left(SINR > \beta\right) E(M), 0 < E(R) \le W, \tag{25}$$

as the expectation of communication throughput R. Thus, the optimal FN deployment should be the Poisson distribution with density ${\lambda_f}^* = \arg\min_{\lambda_f} \left(E\left(R\right) = W\right)$.

Due to the complexity of $\Pr(SINR > \beta)$, we cannot find the optimal ${\lambda_f}^*$ in close-form solution. Fortunately, as the monotonous increase for $\Pr(SINR > \beta)$ with FN density λ_f, we design the following searching algorithm to find the optimal value of FN density ${\lambda_f}^*$ for a given λ_d and λ_a.

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 $E(R)$ based on ${\lambda_f}^0$

4: **if** $E(R) < W$ **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** $E(R) < W$ **then**

14: set $a = {\lambda_f}^*$

15: **else**

16: set $b = {\lambda_f}^*$

17: **end if**

18: **end while**

19: **output** ${\lambda_f}^*$

V. Numerical Results and Discussions

In this section, we first validate the accuracy of our theoretical analysis by comparing equations (12) and (24) with the simulation results in different scenarios. Then we give the optimal FN deployment under different TN densities. We consider an IoT network where TNs and FNs are distributed in PPP with densities. The network coverage is set as a circular area with radius of 150 m, and the radius of interference area D_0 is set as 50 m. TN transmit power P equals to 20 dBm, and the path loss model is $g(d) = d^{-2.5}$ [13]. We set the noise power σ as -104 dBm. The transaction length L is 256 bits [16], and the transaction arrival density is $\lambda_a = \frac{1}{1800} s^{-1}$ [18]. The total considered time is set to 10000 s.

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 densities. For analytical result, it is computed from equation (20). 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. 3 shows the probability $\Pr(SINR > \beta)$ for both analytical results and simulations with different TN densities under SINR threshold parameter $\beta = -15\mathrm{dB}$ and $\beta = -9\mathrm{dB}$. From this figure, we can see that the curves of analytical results for both β match closely to those of simulations. Specifically, the successful rate for analytical results and simulations is 76% and 77% respectively when the TN density equals to 1.0×10^5 and $\beta = -15\mathrm{dB}$, implying that the difference between the analytical results and simulations is trivial. Moreover, as expected, under both $\beta = -15\mathrm{dB}$ and $\beta = -9\mathrm{dB}$ scenarios the probability $\Pr(SINR > \beta)$ decreases with the TN density due to the increasing interference.

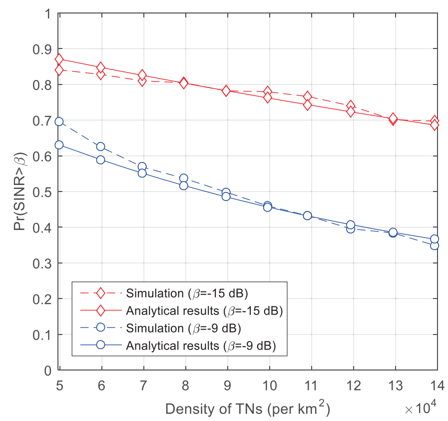

Fig. 3. Comparisons of $\Pr(SINR > \beta)$ vs. TN density (FN density is 320 km^2).

Next, we evaluate the performance of overall communication throughput as a function of TN densities. 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 minutes in Bitcoin [19]), the overall communication throughput in this paper is calculated as: the total data volume that is successfully transmitted in every 10 minutes for all TNs. Due to the limitation of the maximum transaction throughput (MTT) in blockchain, the overall communication throughput will stay unchanged once the transaction throughput achieves the MTT. Fig. 4 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. 4, we can see that the communication throughput for all the four scenarios is increased when the TN density is low. With TN density increasing, the curve with parameters $\beta = -15\mathrm{dB}, \mathrm{MTT} = 7\mathrm{TPS}$, $\beta = -9\mathrm{dB}, \mathrm{MTT} = 7\mathrm{TPS}$ and $\beta = -15\mathrm{dB}, \mathrm{MTT} = 14\mathrm{TPS}$ arrives to the maximum communication throughput sequentially. The curve with parameters $\beta = -9\mathrm{dB}, \mathrm{MTT} = 14\mathrm{TPS}$ 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 $\beta = -9\mathrm{dB}, \mathrm{MTT} = 14\mathrm{TPS}$ is decreased due to the high interference.

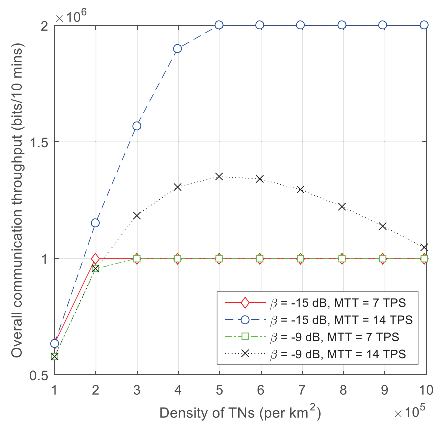

Fig. 4. Comparisons of overall throughput vs. TN density (FN density is 5000 km^2).

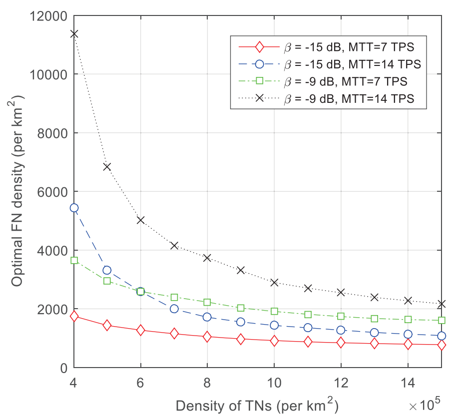

Fig. 5. Comparisons of optimal FN density vs. TN density.

In the last experiment, we investigate the optimal FN deployment with different TN densities. Fig. 5 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 is decreased sharply. The rationale behind is that that the more TNs are deployed, the more transactions need to be transmitted 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, even the number of transactions is increased, the overall throughput is changed slowly, and thus the slow change of the optimal FN density.

VI. Conclusions

In this paper, we established a fundamental analysis model to underpin the blockchain enabled IoT system. We theoretically obtained the distribution of SINR, TDP transmission successful rate as well as overall communication throughput. Then based on the performance analysis, we designed an optimal blockchain full function node deployment to achieve the maximum transaction and communication throughput. Numerical results validated the accuracy of our theoretical analysis (less than 2% error). The framework of the system model and analysis approach establish a foundation for further complex blockchain enabled system performance analysis and protocol design.

References

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

[2] K. C. Darrell Etherington, "Large DDoS Attacks Cause Outages at Twitter, Spotify, and Other Sites," https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/, accessed Sep 20, 2018.

[3] L. H. NEWMAN, "What We Know About Friday's Massive East Coast Internet Outage," https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/, accessed Sep 20, 2018.

[4] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain Challenges and Opportunities: A Survey," *Work Pap.–2016*, 2016.

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

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

[7] M. Iansiti and K. R. Lakhani, "The Truth about Blockchain," *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, 2017.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer Electronic Cash System," 2008.

[9] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng, "When internet of things meets blockchain: challenges in distributed consensus," *arXiv preprint arXiv:1905.06022*, 2019.

[10] O. Onireti, L. Zhang, and M. Imran, "On the viable area of wireless practical byzantine fault tolerance (pbft) blockchain networks," vol. 3, 2019, p. 1.

[11] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng, and J. Yu, "Direct acyclic graph based blockchain for internet of things: Performance and security analysis," *arXiv preprint arXiv:1905.10925*, 2019.

[12] 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 Journal on Selected Areas in Communications*, vol. 27, no. 7, pp. 1029–1046, 2009.

[13] K. Smiljkovikj, P. Popovski, and L. Gavrilovska, "Analysis of the Decoupled Access for Downlink and Uplink in Wireless Heterogeneous Networks," *IEEE Wireless Communication Letters*, vol. 4, no. 2, pp. 173–176, 2015.

[14] T. Bai and R. W. Heath, "Coverage and Rate Analysis for Millimeter Wave Cellular Networks," *IEEE Transactions on Communications*, vol. 14, no. 2, pp. 1100–1114, 2015.

[15] Y. Zhong, T. Q. S. Quek, and X. Ge, "Heterogeneous Cellular Networks with Spatio-Temporal Traffic : Delay Analysis and Scheduling," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, pp. 1373–1386, 2017.

[16] 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 *International Conference on Distributed, Ambient, and Pervasive Interactions*, 2018, pp. 21–34. [Online]. Available: http://link.springer.com/10.1007/978-3-642-39351-8

[17] P. L. Hsu and H. Robbins, "Complete Convergence and the Law of Large Numbers." *Proceedings of the National Academy of Sciences of the United States of America*, vol. 33, no. 2, pp. 25–31, 1947.

[18] 3GPP TR 45.820 v13.10, "Cellular system support for ultra low complexity and low throughput internet of things (CIoT)," 2015.

[19] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: A Scalable Blockchain Protocol," in *USENIX Symposium on Networked Systems Design and Implementation*, 2016, pp. 45–59. [Online]. Available: http://arxiv.org/abs/1510.02037