Blockchain-enabled Wireless IoT Networks with Multiple Communication Connections

Jingxin Zhu[‡*], Yao Sun[†], Lei Zhang[‡] *Senior Member, IEEE*, Bin Cao[§], Gang Feng[†] *Senior Member, IEEE*, Muhammad Ali Imran[‡] *Senior Member, IEEE*

[*] Glasgow College, University of Electronic Science and Technology of China, Chengdu, China

[†] National Key Lab. on Communications, University of Electronic Science and Technology of China, Chengdu, China

[‡] James Watt School of Engineering, University of Glasgow, Glasgow

[§] Institute of Network Technology, Beijing University of Post and Telecommunications, Beijing, China

Email: zhujingxin@std.uestc.edu.cn, sunyao@uestc.edu.cn, lei.zhang@glasgow.ac.uk, caobin65@163.com, fenggang@uestc.edu.cn, Muhammad.Imran@glasgow.ac.uk

***Abstract*—Blockchain-enabled wireless network has been recognized as an emerging network architecture to be widely employed into the Internet of Things (IoT) ecosystems for establishing trust and consensus mechanisms without the involvement of a third party. However, the uncertainty and vulnerability of wireless channels among the IoT nodes may pose a serious challenge to facilitate the deployment of blockchain in wireless networks. In this paper, we first present a generic system model for blockchain-enabled wireless networks with multiple communication connections, where the number of communication connections between a client IoT node and the blockchain full nodes can be any arbitrary positive integer to satisfy different security requirements. Based on the proposed spatial-temporal network model, we theoretically calculate the transmission successful probability and the required communication throughput to support a wireless blockchain network. Finally, simulation results validate the accuracy of our theoretical analysis.**

I. Introduction

Blockchain is a revolutionary ledger store system offers a decentralized architecture and strong tamper-proof ability, thanks to the cryptographic and consensuses mechanisms advances in past decades. It was originally proposed as a backbone technology for the bitcoin cryptocurrency [1]. It has the potential to transform the way in which we share information and reshapes the future digital economy and society widely ranging from Internet of Things (IoT), energy, transportation, finance service, healthcare, identity management, etc [2], [3].

Various consensus algorithms have been proposed to satisfy the requirement of diversified scenarios [1], [4], [5] and guarantee the security of data base. Proof of Work (PoW) [1] and Proof of Stake (PoS) [6] are two typical consensus mechanisms. PoW is the originally proposed consensus mechanism applied in bitcoin, which is based on the competition of computing power, i.e., the node with the highest computing power has the best probability to win the right to generate a new block to record data, rewarded by bitcoins and transaction fees. Rather than depending on the computing power, in PoS, the probability to win the right is determined by coin age, which is a specific property defined in the scenario of blockchain. The value of coin age is obtained by the value of coins a node holds times the lifetime.

A typical blockchain is usually applied in a wired network with high stability and security of communication among the nodes in the consensus network. Blockchain deployment in wireless is foreseeable in the near future when the Always-Connected device is de facto perspective. Due to the openness of the wireless communication channel and the broadcast nature of radio propagation, the system may be attacked by malicious users. Thus, applying blockchain in a wireless network can significantly enhance the security of wireless networks.

Despite the advantages of applying blockchain to wireless networks, there are some issues to be addressed for establishing the blockchain-enabled wireless network. A particular challenge is how will the uncertainty and vulnerability of the wireless connections between the client IoT nodes and blockchain full nodes affects the overall security level of blockchain. In addition, it is not clear how much communication throughout is required to achieve a secure blockchain transaction in the wireless connected networks. The authors in [7] describe a detailed model for the blockchain-enabled wireless IoT system, while in this model, all performance analysis is based on the single wireless connection between the client IoT node and the full node, which can be easily attacked by either block the link between them of the full node. In addition, due to the channel randomness, the security performance can be bottled by the single connected wireless channel seriously [8]. Therefore, multiple connections among the client and full node should be analysis to satisfy security requirement in practice, which to the best of the authors' knowledge, is not available in the literature.

In this paper, we first present a general model for blockchain-enabled wireless IoT networks with multiple connections among nodes. Then we theoretically calculate the transmission successful probability and communication throughput with the given model. The required communication resource to securely

This work was supported by the National Science Foundation of China under Grant number 61871099 and the U.K. Engineering and Physical Sciences Research Council (EP/S02476X/1).

run a wireless blockchain network is also derived to give a practical guide for the blockchain full node deployment. We conduct simulations to verify the accuracy of our theoretical analysis. The difference between the simulation and analytical results under the typical circumstances is 3%, which clearly validate the theoretical analysis in the generic model.

II. System Model

In this section, we first describe a blockchain-enabled network model with the consideration of the security requirement and then present a wireless communication model based on the spatial-temporal domain characteristics.

A. Blockchain-enabled Network Model

Consider a blockchain-enabled network model as shown in Fig. 1, where two types of nodes: IoT clients represented by single-function nodes (SNs), and full-function nodes (FNs) are located. SNs are the majority of nodes in this model and supported by the blockchain functionality for transactions[1]. SNs can only transmit transaction information because of their low-power, and small storage. For each SN, it can be in active or idle mode. An SN is active when it is transmitting information, or the SN is idle. The detailed characteristics of the SN mode in the time domain are described in the system model in the next section. FNs are the nodes to support the blockchain protocols. In this network, FNs are responsible to confirm and store the information transmitted from SNs and build new block to the chain. Therefore, FNs are required to be with high computing ability and large storage. For the consideration of security, FNs are connected with each other via either high-speed wireless or wired links. In addition, FNs are connected with SNs via a wireless connection, as shown in Fig. 1.

The transmission process among the network can be described as follows. In this paper, we focus on the uplink transmission from SN to FN, however, the downlink transmission can be analyzed in a similar method by using the proposed model and derivations. When a package arrives at an SN, it broadcasts the information to FNs. In order to guarantee the security of the transmission, as many as FNs should receive the information. Clearly, it is easier to guarantee a secure transmission with a larger number N for all the N FNs will share the information with the whole network. However, such redundant connections will cause a higher communication resource requirement. In this paper, the model can be applied in circumstances requiring any degree of security. Without loss of generality, we assume it is received by N FNs and $N \geq 1$ and $N \in \mathbb{N}$, i.e., we assume that it is secure only the transaction successfully received by N FNs. The security level would be enhanced by increasing the value of N. Take the example of $N = 2$ as shown in Fig. 1. When the information transmitted by SN is received by two FNs, the transmission is secure since any one of the links attacked by a malicious user will not affect the success of the transaction. In this paper, assume that the N closest FNs to the SN could receive the information of the SN since they could receive the largest signal power.

[1]Note that transactions can be any kind of information exchange this is to be recorded into a ledger for recording.

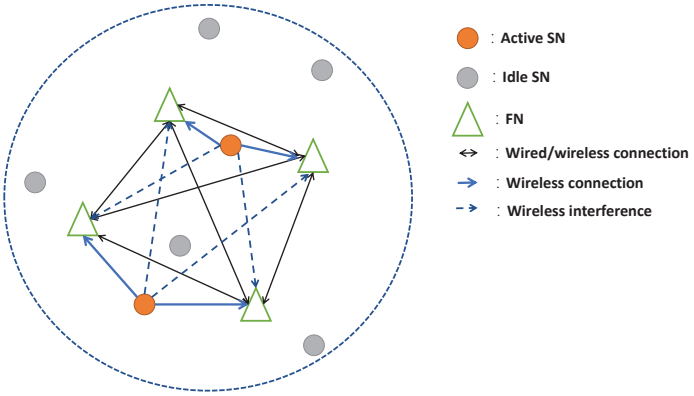

Fig. 1. Blockchain-enabled network model under the circumstance of $N = 2$

Note that Fig. 1 shows a network snap-shot, and the state (active or idle) of SNs can be changed dynamically. In this work, we theoretically analyze the transaction throughput C, which is the number of the packet confirmed in a unit time, with the unit of transactions per second (TPS). For a specific blockchain network, its maximum transaction throughput is a limited value. Usually, the performance of a wireless blockchain is described by communication throughput R, which is the amount of data transmitted in a unit time, with the unit of bits per seconds (bps). In our model, the same packet of information is transmitted to N FNs at the same time, then the communication throughput in this network can be calculated as follows,

$$R \geq NLC, \tag{1}$$

where L is the length for a packet. As the value of C is limited by blockchain protocols, there is a maximum value for the required communication throughput in this network.

B. Wireless Communication Model

We describe the blockchain-enabled wireless communication model by assuming the spatial-temporal distribution of nodes. First, in the spatial domain, all SNs and FNs are assumed to be distributed as a homogeneous Poisson Point Process (PPP) with density λ_s and λ_f respectively. For practical consideration, there is a minimum distance d_{min} between SNs and FNs. In addition, we assume an interference distance d_I. SNs can interfere FNs with distance within d_I. Then, in the temporal domain, SNs are in active mode as transmitting information to FNs. Usually, the length L for each packet is very short (e.g., 1KB in Bitcoin [9]), thus the active time t of SNs can be very small, and thus $t \ll T$ holds. Therefore, the number of the arrived packet of information during a given time can be considered as a Poisson distribution with parameter $\lambda_a T$. Considering a circular with the center of an FN and the radius of d_I, there are several SNs inside this circular. At any specific time, some of SNs are active, which are transmitting

information to their N closest FNs, and others are idle. In this work, we consider that all SNs share the same bandwidth resource, thus interference should be taken into account.

In this model, it is assumed that the transmission from SN to FN is successful when the information is received by N FNs. Thus, for each FN, the received Signal-to-Interference-plus-Noise-Ratio (SINR) should be larger than a threshold β. The process of the transmission from SN to the N FNs can be analyzed in the same way. Thus, in the following we analyze the transmission link between the SN and the kth nearest node FN k. The signal received by FN k experiences the path loss $g(D_{k1})$, where D_{k1} is the distance between FN k and the SN. Denote by N_I the number of active SNs within the distance of d_I from the FN. The N_I active SNs interference the transmission from the SN to the FN. Therefore, the SINR received by FN k can be expressed as

$$SINR_k(D_{k1}, N_I, \mathbf{D}_{k2}) = \frac{Pg(D_{k1})}{\sum_{i=1}^{N_I} Pg\left(D_{k2}^{(i)}\right) + \sigma}, \quad (2)$$

where $\mathbf{D}_{k_2} = \left[D_{k2}^{(1)}, Dk_{k2}^{(2)}, ..., Dk_{k2}^{(N_I)}\right]$ is the distance vector for all interference SNs with FN k, and σ is the noise power. In this work, successful and secure transmission of SN should satisfy $SINR_k > \beta$ for all $k = 1, 2, ..., N$. For convenience, the frequently used notations are summarized in Table I. Note that, in this paper, we use capital letters to represent random variables and the corresponding lowercase letters to represent the value of random variables.

TABLE I
FREQUENTLY USED NOTATIONS

Notation	Definition
R	communication throughput
C	transaction throughput
D_I	the radius of the interference area
k	the order of serving FN
D_{k1}	distance between SN and FN k
$\mathbf{D}_2$	distance vector of all interference SNs (a vector)
$D_2^{(i)}$	distance between interference SN i and the FN
λ_s	SN density
λ_f	FN density
λ_a	blockchain transaction arrival rate
N_{SN}	the number of total SNs
N_I	the number of interference SNs
T	the total considered time
L	the packet length of each blockchain transaction
P	SN transmit power
$g(d)$	channel path loss model (a function of distance)

III. Performance Analysis in Blockchain-enabled Wireless networks

In this section, we theoretically analyze the performance in the blockchain-enabled wireless networks through the analysis of SINR for each serving FN, the transmission successful probability, and communication throughput. In detail, we first derive the probability density function (PDF) of SINR for the N serving FNs respectively. Based on the PDF, we calculate the transmission successful probability and the expectation of required communication.

A. Probability Density Function of SINR

We start with the derivation of PDF of SINR. In order to derive a general form of SINR distribution for the N FNs, we analyze the SINR for FN k. For a specific SN and its corresponding FN k, the desired signal power $S_k = Pg(D_{k1})$, where P is set as a constant value in this paper, thus the PDF of S is only related to D_{k1}. Proposition 1 gives the general PDF of D_{k1} for any k.

Proposition 1. *The PDF of SINR between a specific SN and its corresponding FN k is*

$$f_{D_{k1}}(d_{k1}) = 2\pi\lambda_f d_{k1}\exp\{-\lambda_f\pi\left(d_{k1}\right)^2\} + \sum_{i=2}^{k} \frac{\left(2(\pi\lambda_f)^{i-1}(d_{k1})^{2i-3}\exp\{-\lambda_f\pi\left(d_{k1}\right)^2\}\{\lambda_f\pi\left(d_{k1}\right)^2+1-i\}\right)}{(i-1)!}. \quad (3)$$

Proof: FN k for a specific SN is the kth nearest FN for the SN. Let D_{k1} be the distance between SN and its corresponding FN k. We calculate the probability that $D_{k1} > d_{k1}$. The number Q of the FNs locating inside the circle can be $0, 1, 2, ..., k-1$. As mentioned in Section II. B, FNs are distributed with parameter λ_f, thus $\Pr(D_{k1} > d_{k1}) = \sum_{i=1}^{k}\Pr(Q = i-1) = \exp\{-\lambda_f\pi\left(d_k1\right)^2\} + \sum_{i=2}^{k}\frac{\{\lambda_f(\pi d_{k1})^2\}^{i-1}\exp\{-\lambda_f\pi(d_{k1})^2\}}{(i-1)!}$. Therefore, the cumulative distribution function of D_{k1} can be calculated as follows,

$$F_{D_{k1}}(d_{k1}) = 1-\Pr(D_{k1}>d_{k1}) = 1-\exp\{-\lambda_f\pi\left(d_{k1}\right)^2\} - \sum_{i=2}^{k}\frac{\{\lambda_f\left(\pi d_{k1}\right)^2\}^{i-1}\exp\{-\lambda_f\pi\left(d_{k1}\right)^2\}}{(i-1)!}. \quad (4)$$

Then the PDF of D_{k1} can be derived as,

$$f_{D_{k1}}(d_{k1}) = \frac{d\big(F_{D_{k1}}(d_{k1})\big)}{d(d_{k1})} \quad (5)$$

■

For a specific SN, the PDF of the received signal S_k from its corresponding FN k can be derived based on Proposition 1 as,

$$f_{S_k}\big(S_k = Pg(d_{k1})\big) = f_{D_{k1}}(d_{k1}), \quad (6)$$

where $f_{D_{k1}}$ is given in (3).

Then we analyze the PDF of received interference signal S_I. PDF of S_I is the same for the N serving FNs since it is only related to N_I, the number of interference SNs, and $\mathbf{D}_2$, the distance between interference SNs and the serving FN, where $d_2^{(i)} < D_I$ for $i = 1, 2, ..., N_I$. The received interference signal

can be presented as $S_I = \sum_{i=1}^{N_I} Pg\left(D_{k2}^{(i)}\right)$, where P is the transmission power. Since the distance between the serving FN and the specific SN does not influence the PDF of S_I, the PDF of S_I can be obtained in [7], which is based on the Poisson distribution of information arrival and SN spatial distribution. The expression of PDF of S_I is shown below,

$$\begin{aligned} f_{S_I}(S_I = \sum_{i=1}^{N_I} Pg\left(D_{k2}^{(i)}\right)) &= f_I(N_I = n_I, \mathbf{D}_2 = \mathbf{d}_2) \\ &= f_{N_I}(n_I)\left(\frac{2}{(D_0)^2}\right)^{n_I} \prod_{n=1}^{n_I} d_2^{(n)}. \end{aligned} \tag{7}$$

For a specific SN, the SINR$_k$, the SINR received by FN k, is related to the received signal by FN k and the interference signal, thus the PDF of SINR$_k$ can be expressed as

$$\begin{aligned} &f_{SINR_k}(D_{k1} = d_{k1}, N_I = n_I, \mathbf{D}_2 = \mathbf{d}_2) \\ &= f_{S_k}(D_{k1} = d_{k1}) f_{S_I}(N_I = n_I, \mathbf{D}_2 = \mathbf{d}_2), \end{aligned} \tag{8}$$

where f_{S_k} and f_{S_I} are given in (6) and (7), respectively.

B. Transmission Successful Probability

In this model, we assume that a transmission is successful only when the information transmitted by a specific SN is received by N FNs (N can be any integer). When the received SINR$_k$ for kth serving FN is larger than the threshold β, it can be considered that the FN receives the information successfully. Therefore, in the work, for a specific SN, when the N SINR$_k$($k = 1, 2, ..., N$) are all larger than the threshold β, the transmission is successful.

In this model, the receiving successful probability for each FN is independent with each other. The only relationship to FN is their relative position, i.e., the receiving successful probability of an FN varies with the position of this FN. Therefore, an FN successfully receives the information would not influence the receiving successful probability for other FNs. Then we calculate the probability of successful transmission which can be expressed as

$$\begin{aligned} \Pr(E_N) &= \Pr(SINR_1 > \beta, ..., SINR_k > \beta, ...SINR_N > \beta) \\ &= \prod_{k=1}^{N} \Pr(SINR_k > \beta), \end{aligned} \tag{9}$$

where E_N means the event that the information is successfully received by N FNs, and $\Pr(SINR_k > \beta) = \iiint_{\Omega_k} f_{SINR_k} d\Omega_k$, where Ω_k is the area of $(D_{k1}, N_I, \mathbf{D}_2)$ that satisfies $SINR_k(D_{k1}, N_I, \mathbf{D}_2) > \beta$. In order to calculate the transmission successful probability, first calculate the probability for each SINR$_k$ that satisfies $SINR_k > \beta$. SINR$_k$ is given in (8), thus the only thing to do is to find the ω_k for each serving FN. For each D_{k1}, although the distribution in the spatial domain is not the same, the satisfied range of them is the same, which is $[D, D_I]$. It is reasonable to assume that SINR$_k$ cannot be larger than β when $D_{k1} > D_I$. In addition, as we mentioned in Section III. A, the distribution of D_{k2} and N_{kI} does not vary with the position of FNs (generally denote as D_2 and N_I), thus the range for D_{k2} and N_{kI} for each serving FN is the same. Then the derivation in [7] can be generalized to satisfy the model in this work, thus the equation for each serving FN is as follows,

$$\begin{aligned} \Pr(SINR_k > \beta) &= \iiint_{\Omega_k} f_{SINR_k} d\Omega_k \\ &= \int_{d_{k1}=d_{min}}^{D_I} f_{D_{k1}}(d_{k1})\, \Phi(\xi(d_{k1}))\, d(d_{k1}). \end{aligned} \tag{10}$$

where $\xi(d_{k1}) = \frac{\frac{Pg(d_{k1})-\sigma}{\beta} - \mu_{kI}}{\delta_{kI}}$, Φ is the cumulative density function of standard normal distribution, and for the f_{S_I} is the same for each serving FN, the expressions of parameter μ_{kI} and δ_{kI} relating with the interference signal are the same for each FN k. Denote them as μ_I and δ_I, their expressions can be obtained in [7].

The receiving successful probability for the N serving FNs can be obtained with function $f_{D_{k1}}$, and other given parameters. Then the transmission successful probability (9) can be calculated.

C. Communication Throughput

With the transmission successful probability, then we can calculate the communication throughput in this wireless blockchain network. Based on (1), we can write the communication throughput R as follows,

$$R = LN \cdot \Pr(E_N)\left(\sum_{i=1}^{N_{SN}} M_i\right),\ 0 \le R \le W \tag{11}$$

where N_{SN} is the total number of SNs in this networks, M_i is the number of packet for information transmitted by the ith SN, and W is the maximum value of communication throughput in this networks where the transaction throughput reaches the maximum value and can be expressed as follows,

$$W = LNC_{max}T, \tag{12}$$

where C_{max} is the maximum value of transaction throughput.

It can be seen clearly in (11), L, N, N_{SN}, and $\Pr(E_N)$ are constants for given λ_s and λ_f. While M_i is a set of independent identically PPP distributed random variables with parameter $E(M_i) = \lambda_a T$ and $D(M_i) = \lambda_a T$. Denote $M = \sum_{i=1}^{N_{SN}} M_i$, as N_{SN} is a large number, M is a random variable with normal distribution $N(\mu_M, {\delta_M}^2)$ [10]. Therefore, the communication throughput R is also a random variable with normal distribution $N(\mu_R, \delta_R^2)$ when $0 \le R \le W$. Then we can have

$$\mu_R = LN\Pr(E_N)\mu_M = LN\Pr(E_N)N_{SN}\lambda_a T, \tag{13}$$

$$\delta_R = LN\Pr(E_N)\delta_M = LN\Pr(E_N)\sqrt{N_{SN}}\lambda_a T. \tag{14}$$

In order to analyze the performance of the networks directly, instead of calculating R, we can calculate $E(R)$, which can be calculated easily as follow,

$$E(R) = \min\{\mu_R, W\} = \min\{LN\Pr(E_N)N_{SN}\lambda_a T, W\}. \tag{15}$$

With (15), we can analyze the relationship between the communication throughput and the density of SNs and FNs respectively. Theoretically, as expressed in (15), the communication throughput has a limitation as the blockchain transaction throughput is limited. Considering the expression for $\Pr(E_N)$ in (9) and combining the practical, for given L, N, N_{SN}, λ_s in the given environment, it can be found that within a range, the communication throughput increases with λ_f as the increasing of transaction throughput. As the λ_f reaches a value, the transaction throughput reaches the limitation, then the communication throughput reaches its maximum value W. Then, the communication throughput stays unchanged with λ_f. Therefore, in this network, we can find the optimal node deployment ${\lambda_f}^*$ to satisfy the maximum communication throughput without wasting FNs, where ${\lambda_f}^*$ is the minimum value of λ_f to allow the communication throughput R reaches W. While compare (15) and (12), it can be found that ${\lambda_f}^*$ should satisfy the following equation,

$$\Pr(E_N) N_{SN} \lambda_a = C_{max}. \tag{16}$$

Since $\Pr(E_N) \leq 1$, the right equation in (16) has its limitation which is determined by N_{SN}. Therefore, when the value of N_{SN} is considerable small, communication throughput in this network keeps increase with λ_f, thus there is no ${\lambda_f}^*$ under this circumstance.

In addition, when the value of N_{SN} is large enough for the existence of ${\lambda_f}^*$, though there is no close-form for the calculation of ${\lambda_f}^*$ because of the complexity of the expression for $\Pr(E_N)$, the approximate value of ${\lambda_f}^*$ can be obtained by using algorithm, such as method of bisection, steepest descent method and other methods.

IV. Numerical Results and Discussions

In this paper, we assume that the transmission of information can be seen as a successful transmission when the information is received by N FNs, where N can be any positive integer. In this simulation, we verify the accuracy of the proposed theatrical analysis with $N = 2$ and $N = 3$, respectively. In the network with $N = 2$, the radius of interference is $D_I = 70$ m, and $D_I = 90$ m for $N = 3$, because the threshold for modulation and demodulation is looser with larger N. Other simulation parameters in the two networks are the same. The radius of the considered area is 150 m, the transmit power P is 20 dBm, the path loss model is $g(d) = d^{-2}$ [11], the total time T is 10000 s, the transaction packet length L is 256 bits [9], the transaction arrival density λ_a is $\frac{1}{1800} s^{-1}$ [12], the noise power σ is -104 dBm.

A. Validation of Theoretical Results

In this experiment, we compare the theoretical results with simulation results to validate the accuracy of transmission successful probability in (9). The theoretical results are obtained by using equations in Section III. A and III. B. In the simulation platform, if the two values of SINR for the two serving FN for a specific SN, are larger than β simultaneously, the transmission is considered successful. If the requirement is not satisfied, the transmission is considered a failure.

In the first experiment, we examine the transmission successful probability with fix FN density and varying SN density. Fig. 2 shows the result for the network with $N = 2$, and $N = 3$ respectively. For the circumstance of $N = 2$, with $\lambda_f = 526$ / km^2 and $\beta = -3$ dB, the average absolute value of the difference between the simulation results and theoretical results is 1.9% which verifies the effectiveness of the derivations. Then, with $\lambda_f = 304$ / km^2 and $\beta = -9$ dB in the circumstance $N = 3$, the absolute difference here is 3.446%. Therefore, the trivial difference in the circumstance of the various value of N, λ_f, and β verify that the theoretical equation can work for the fix FN density and varying SN density. Moreover, the transmission successful probability decreases with the SN density, and the slope of the curve also decreases as expected from theoretical analysis.

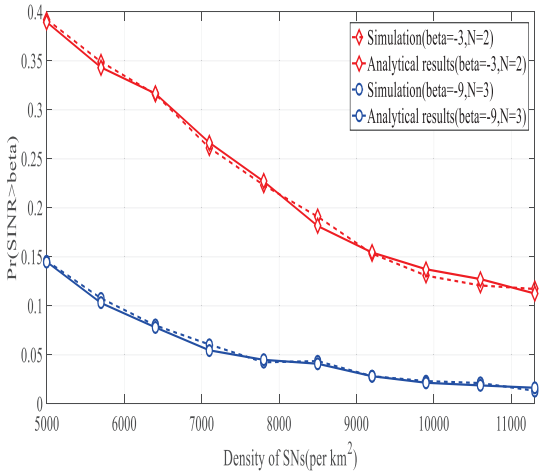

Fig. 2. Comparisons of $\Pr(E_N)$ vs. SN density (FN density is 526 / km^2 for $N = 2$ and 304 / km^2 for $N = 3$).

In the second experiment, with fixed SN density, we re-examine the transmission successful probability with varying FN density. Fig. 3 validate the analytical results with the average absolute difference with simulation and analytical results 1.79% for $N = 2$, and 2.1% for $N = 3$. Under the circumstance of $N = 2$, SN density is 2052 / km^2 and $\beta = -3$dB. In the network with $N = 3$ with $\lambda_s = 6908$ / km^2. Moreover, in both two systems, the transmission successful probability increases with the density of FN because of the decreased distance between FNs and SNs.

B. Communication Throughput Analysis

In the third experiment in this paper, as discussed in Section III.C, we use (15) to present communication throughput. For calculation, $T = 10$ min, since in Bitcoin, a new block is generated about every 10 minutes [13]. We calculate communication throughput for both $N = 2$, and $N = 3$. Fig. 4 shows the calculation results of communication throughput for $\lambda_f = 526$ / km^2), $\beta = -3$ dB when $N = 2$, and $\lambda_f = 304$ / km^2),

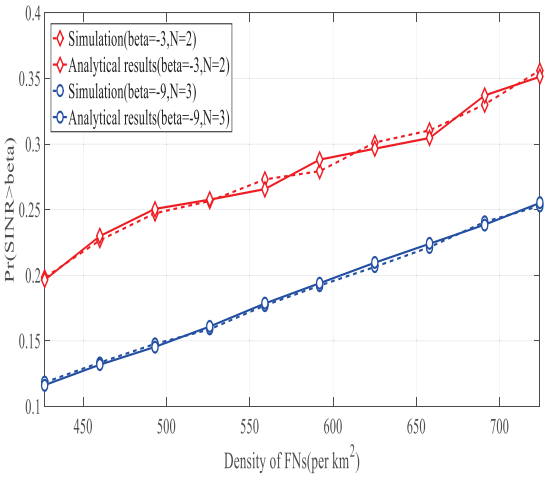

Fig. 3. Comparisons of $\Pr(E_N)$ vs. FN density (SN density is 2052 / km^2 for $N = 2$, and 6908 / km^2 for $N = 3$).

$\beta = -9$ dB when $N = 3$. For both situation, $C_{max} = 7$ TPS. In Fig. 4, it can be seen that the communication throughput decreases with SN density due to the increasing high interference. Analyzing more carefully, it can be found that the rate of decreased communication throughput between the same difference of SN varies significantly. For example, when $N = 2$, the slope between the third point and the fourth point is much steeper than the others, and the curve between the fifth and sixth point is nearly a straight line, which means that the communication throughput is nearly the same when SN density between 7599 / km^2) and 8289 / km^2). Therefore, through this analytical analysis, in practice, we can find a range of SN density where SN density increases a lot while communication throughput does not decreases significantly, so we can increase the SN density in the network without significant decrease of communication throughput. This provides valid theoretical guidance for the blockchain-enabled network design.

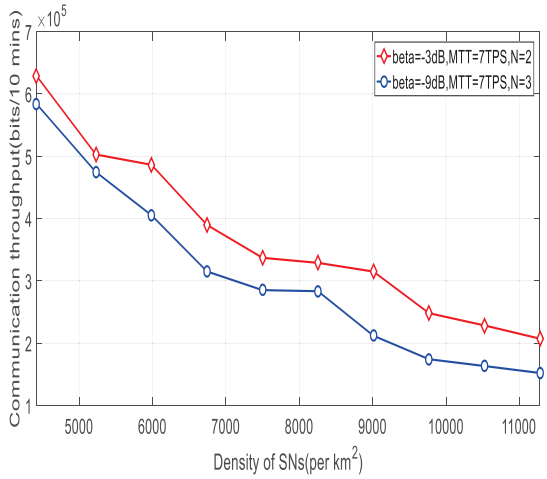

Fig. 4. Comparisons of overall throughput vs. SN density (FN density is 526 / km^2 for $N = 2$ and 304 / km^2 for $N = 3$).

V. Conclusions

In this paper, we established a framework for the blockchain-enabled wireless networks with multiple communication connections between IoT client and full nodes. In this model, the number of connections can be any positive integer to meet the security level requirement. Based on the spatio-temporal characteristic of the networks, we present the probability density function of SINR for an SN that successfully connected with arbitrary number FNs. Given the PDF of SINR, we calculate the transmission successful probability and the expectation of communication throughput. In addition, we discussed the relationship between communication throughput and node deployment. Simulations validate the accuracy of the theoretical analysis. The framework and performance analysis established in this paper can be used in the design of blockchain-enabled wireless networks with the various security requirements.

References

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

[2] 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," *IEEE Network*, March 2019. [Online]. Available: http://eprints.gla.ac.uk/181576/

[3] B. Cao, M. Li, L. Zhang, Y. Li, and M. Peng, "How does csma/ca affect the performance and security in wireless blockchain networks," *IEEE Transactions on Industrial Informatics*, 2019.

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

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

[6] G. BitFury, "Proof of Stake versus Proof of Work," https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf, Sep. 2015, [Online; accessed 28-September-2018].

[7] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-enabled wireless internet of things: Performance analysis and optimal communication node deployment," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[8] H. Xu, L. Zhang, Y. Liu, and B. Cao, "RAFT based Wireless Blockchain Networks in the Presence of Malicious Jamming." *IEEE Wireless Communication Letter*, 2020.

[9] 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

[10] 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.

[11] 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.

[12] 3GPP TR 45.820 v13.10, "Cellular system support for ultra low complexity and low throughput internet of things (CIoT)," 2015.

[13] 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