RAFT Based Wireless Blockchain Networks in the Presence of Malicious Jamming

Hao Xu, Lei Zhang, *Senior Member, IEEE*, Yinuo Liu, and Bin Cao, *Member, IEEE*

***Abstract*—Blockchain shows great potential to be applied in wireless IoT ecosystems for establishing the trust and consensus mechanisms without central authority's involvement. Based on RAFT consensus mechanism, this letter investigates the security performance of wireless blockchain networks in the presence of malicious jamming. We first map and model the blockchain transaction as a wireless network composed of uplink and downlink transmissions by assuming the follower nodes' position as a Poisson Point Process (PPP) with selected leader location. The probability of achieving successful blockchain transactions is derived and verified by extensive simulations. The results provide analytical guidance for the practical deployment of wireless blockchain networks.**

***Index Terms*—Wireless blockchain network, RAFT, security analysis, private blockchain, jamming.**

I. Introduction

BLOCKCHAIN is a revolutionary record/ledger store system that offers users a decentralized architecture and strong tamper-proof ability, thanks to the cryptographic and consensuses mechanisms advances in past decades. It has been widely recognized that blockchain has the potential to transform how we share information and reshapes the future digital economy and society widely ranging from Internet of Things (IoT), energy, transportation, finance service, healthcare, etc. [1].

The consensus mechanisms are the ground basis of blockchain for establishing trust and agreement without any third party involvement. Unlike Proof of Work (PoW) [2] and Proof of Stacks (PoS) [3] based public chains [4], the private or consortium blockchain, which has wider applications, uses other consensus mechanisms rather than PoW (or PoS) to avoid high costs of computation, low transaction throughput and long confirmation delay, etc. [1]. Besides, such a network requires a more efficient protocol to allow its existence among wirelessly connected IoT devices and other thin-clients, such as mobile phones. Paxos [5], RAFT [6] and Byzantine Fault Tolerance (BFT) [7] are representative low complexity protocols may be used in wireless connected low-complex device developed for the distributed system with unreliable nodes. The consensus of such a network will be made if the majority votes successfully through the communications among the nodes in the consensus networks [8]. In other words, if too many honest votes fail, due to communication faults or false information by malicious users, the agreement on this transaction will not happen. Hence the blockchain synchronization will fail.

Depends on whether the consensus network has malicious (or Byzantine) users that may send fake information to others, we have BFT [7], which prevents dishonest nodes rigging the decision, and the Crash Fault Tolerance (CFT) [5] consensus mechanism, which does not allow the existence of Byzantine nodes in the network through strict access control but may have communication links failures. The BFT is not necessary to the private consensus network due to reinforced identification check, whereas, RAFT based CFT is the most demanding feature for faster and less complicated consensus.

In the permissioned private blockchain, all nodes that have the right to vote are honest, so the problem of getting accordance with the peer-to-peer network is the crash tolerance. Therefore the threat will be communication failure among the nodes. To mediate the complexity of phase states, RAFT came into public view with its concise definition, comparable performance as Paxos [5], [6]. RAFT categorizes nodes into two term-time roles (term of service), one leader and many followers. The leader communicates with the followers through downlink (DL) and uplink (UL) transmissions. When the majority has voted and been successfully received by the leader, the transaction is marked as a success, and the transaction will be inserted into the blockchain. In order to build a RAFT consensus algorithm among nodes, the leader is often undertaken by a stronger node with higher capabilities such as better reliability and performances (i.e., power, battery life, etc.). The voting, which is the state replication from leader to followers, matters in the sense that either UL or DL communications may not be successful [6].

Blockchain deployment in wireless is foreseeable. In terms of wireless blockchain, take IoT network as an example, where the network is typically a permissioned and dedicated network, the quorum permission is top priority comparing with trojan threats. Therefore, given the fact of wireless massive low complexity IoT applications are emerging and there is no research except Sun's work [9]. Using his theory, it turns out that RAFT can be a feasible solution under the circumstance of IoT to blockchain-enabled IoT ecosystems under the assumption of Y.Sun's assessment of wireless IoT Blockchain performance. Note that the scheme proposed here is for private chain and no Byzantine node is allowed. However, the wireless connection among the leader and the followers can be vulnerable due to wireless channel fading and un-permitted malicious jammers. Either UL or DL failure will cause specific voting failure, thus lower transaction success rate. In addition, although no

Manuscript received December 1, 2019; accepted January 30, 2020. Date of publication February 4, 2020; date of current version June 10, 2020. This work was supported in part by the U.K. Engineering and Physical Sciences Research Council under Grant EP/S02476X/1, in part by the National Natural Science Foundation of China under Grant 61701059 and Grant 61941114, and in part by the Chongqing Technological Innovation and Application Development Projects under Grant csts2019jscx-msxm1322. The associate editor coordinating the review of this article and approving it for publication was P. Li. *(Corresponding author: Lei Zhang.)*

Hao Xu and Lei Zhang are with the School of Engineering, University of Glasgow, Glasgow G12 8QQ, U.K. (e-mail: h.xu.2@research.gla.ac.uk; lei.zhang@glasgow.ac.uk).

Yinuo Liu is with the School of Maths and Statistics, University of Glasgow, Glasgow G12 8QQ, U.K. (e-mail: y.liu.4@research.gla.ac.uk).

Bin Cao is with the State Key Lab of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: caobin65@163.com).

Digital Object Identifier 10.1109/LWC.2020.2971469

Byzantine node is allowed in private blockchain, malicious users can exist in the network to prevent the consensus being achieved among the nodes through spectrum jamming due to the openness of the wireless channel. Note that the jammers are un-permitted thus do not belongs to the consensus network and it has no right to vote. Thus, the success rate of the blockchain transactions in the presence of radio jamming is a critically important topic to be explored for the practical network deployment. In [9], the authors first proposed the wireless connected blockchain system and modeled the relationship of communication throughput and transaction throughput, and the optimal Full Node (FN) deployment is derived. However, to the best authors' knowledge, there is no work, which considers the security performance for RAFT based wireless blockchain networks with malicious jamming.

Unlike the traditional communication problems that typically focus on the success of individual communication link, the problem in this letter is shifted to multiple communication links network and the aim is to make sure that at least 51% of the communications links (for both uplink and downlink) of them must be successful, with or without the presence of malicious jamming. To solve this problem, we first map and model the blockchain transaction processing into the wireless DL and UL transmission. Then, the transaction success probability of wireless RAFT blockchain is investigated. Note that the jamming attack can come from both high or low layer. We have used the classic metric SINR as a threshold. Any nodes received a signal below the threshold will be considered as a failure. However, it is worth mentioning that the SINR threshold can be changed to any other communication metrics such as Mean Square Error (MSE) or even Bit Error Rate (BER), etc. The analytical results show the relationship of success probability of wireless blockchain network, the nodes location, and transmitting power. Using the fundamental modeling and analysis, the study is also beneficial to cellular, vehicular network or other wireless blockchain-enabled sensors network [10].

II. System Model

The RAFT-based wireless blockchain network is shown in Fig. 1, where the network is composed of two parts, clients and wireless consensus network. Note that, the two parts are not necessarily separated geographically and Fig. 1 is only an example to illustrate the roles of nodes and the communication network topology. In different business models, the IoT node can choose to be a client or become a voter in the blockchain network by playing a leader or a follower. In other words, the roles of the nodes are exchangeable during RAFT consensus election. In the case of being a client, the node is not a part of the consensus network but sends out transaction requests to the leader to agree with the followers. Then it waits for the confirmation from the blockchain network, where the success consensus will be inserted into the blockchain. Following the requirement of RAFT consensus, the nodes who plays the role of leader and followers are categorized into the FN or voters, as shown in Fig. 1. In general, the consensus is triggered by the request from the clients; thus, the communication is one way. However, the result decided by the consensus network can be sent backward, which is not the focus of this letter.

In this letter, we will only focus on the communications inside the consensus network, where we assume all followers for the consensus networks are evenly distributed in a 2-Dimensional free space with Poisson Point Process (PPP). The procedure of wireless RAFT blockchain consensus is stated as follows. Firstly, the FN (leader) sends out a signal that contains transaction information from clients, via DL broadcasting channel to the follower nodes. Upon the successfully received DL message, the voter (follower) will then confirm its voting message to the leader via multi-access UL channels. We assume that there is no multi-access interference among the followers since in the private blockchain networks, Carrier Sense Multiple Access (CSMA) or centralized radio resource allocation is possible. In fact, the IoT transmission interval can be large enough compared to the radio transmission interval [9]. Thus, the probability of collision can be negligible. Lastly, the FN will count all receipts, and the overall aim is to achieve the consensus, i.e., it receives more than 50% of responses from the followers, and any failure in either DL or UL will result in losing that follower and lower the success rate.

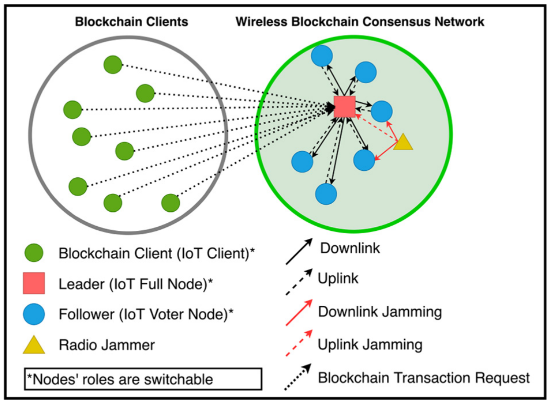
Blockchain Clients
Wireless Blockchain Consensus Network
Blockchain Client (IoT Client)*
Leader (IoT Full Node)*
Follower (IoT Voter Node)*
Radio Jammer
*Nodes' roles are switchable
Downlink
Uplink
Downlink Jamming
Uplink Jamming
Blockchain Transaction Request

Fig. 1. RAFT-based wireless blockchain network.

Suppose the position of the FN is $C_0 = (x_0, y_0)$, which is assumed at the geo-center of consensus network, we assume there is one jammer randomly located around (but not necessarily located inside) the consensus network with a position of (x_1, y_1). For an arbitrary follower node, we assume the location is (*x*, *y*). Thus, its distance to the FN is denoted by $d_F = \sqrt{(x_0 - x)^2 + (y_0 - y)^2}$ and its distance to the jammer is denoted by $d_J = \sqrt{(x_1 - x)^2 + (y_1 - y)^2}$. While the distance between the jammer and the leader can be written as $d_{FJ} = \sqrt{(x_0 - x_1)^2 + (y_0 - y_1)^2}$.

The unified signal model for both UL and DL transmission can be defined as follows:

$$y = Hs + I + N, \tag{1}$$

where $H = h(t)/\sqrt{d^{\gamma}}$ is wireless channel composed of both large scale path loss $PL = d^{-\gamma}$ with d and γ being the distance and path loss exponential factor respectively. *h*(*t*) is the small scale fading factor. Without loss of generality, we assume $h(t) \sim \mathcal{CN}(0, 1)$. s is the signal contains the information of the transaction to be confirmed by the consensus network, *I* is the interference by the jammer and N is the noise with a Gaussian distribution of $N \sim \mathcal{CN}(0, \sigma^2)$.

III. Wireless Blockchain Security Analysis

In the next, we will focus on the derivations of the transaction success rate by modeling the UL and DL wireless communications in the blockchain consensus networks.

A. Downlink Transmission

To have the DL transmission success at any follower, we assume the received SINR (signal-to-interference-plus-noise ratio) is higher than a threshold β_D, i.e.,

$$\text{SINR}_D = E[\frac{P_S|H_S(t)|^2}{d_F^\gamma}]/E[(\frac{P_J|H_J(t)|^2}{d_J^\gamma}+|N|^2)] \geq \beta_D, \tag{2}$$

where E is the expectation operator, $P_S = E\{|s|^2\}$ and $P_J = E\{|I|^2\}$ are the transmitting power of FN and jammer respectively. $H_S(t)$ and $H_J(t)$ are channels from leader to a follower and from the jammer to the follower, respectively. Using the generic channel equation $H = h(t)/\sqrt{d^\gamma}$ and $h(t) \sim \mathcal{CN}(0,1)$, (2) is written as:

$$\frac{P_S}{d_F^\gamma} \geq \beta_D(\frac{P_J}{d_J^\gamma} + \sigma^2). \tag{3}$$

Now let us consider two cases: a noise-limited system without a jammer and an interference-limited system with a jammer. In noise limited case, P_J = 0, and substituting $d_F = \sqrt{(x_0 - x)^2 + (y_0 - y)^2}$ into equation (3), we have $(x - x_0)^2 + (y - y_0)^2 \leq \frac{P_S}{\beta_D}$, which implies that to make the SINR higher than β_D, follower nodes must be located inside the circle at the centre (x_0, y_0) and its radius of $\sqrt{P_S/\beta_D}$.

When the jammer is introduced, due to the strong radiation power of the jammer P_J, we can assume this system is interference limited and thus the noise can be omitted. Substituting $\sigma^2 = 0$ into (3), we can have the following inequality

$$(x - x_D)^2 + (y - y_D)^2 \geq R_D^2. \tag{4}$$

Equation (4) implies that to achieve the SINR threshold, the follower must be outside the jamming circle with its centre at

$$C_{JD} = (x_D, y_D) = (\frac{\alpha_D x_0 - x_1}{\alpha_D - 1}, \frac{\alpha_D y_0 - y_1}{\alpha_D - 1}), \tag{5}$$

and radius is

$$R_D = (\sqrt{\alpha_D(x_0 - x_1)^2 + \alpha_D(y_0 - y_1)^2})/(\alpha_D - 1), \tag{6}$$

where $\alpha_D = (\beta_D P_J)^{\frac{2}{\gamma}}/P_S^{\frac{2}{\gamma}}$. Equation (4) implies that any node inside the circle will be jammed and can not receive the blockchain message from the leader. In the case of the jammed circle (C_{JD}, R_D) is totally inside of the considered area (C_0, R), it is equivalent to use the area of the circle A_{R_D} to represent the the number of failures. Thus, the viable area for DL transmission is the area of the considered circle (C_0, R) except the circular area (C_{JD}, R_D), which is $A_R - A_{R_D}$, where A_R is the area of (C_0, R). Thus, the success rate can be write as $(A_R - A_{R_D})/A_R$. However, when part of the jammed circle (C_{JD}, R_D) is outside (C_0, R), the variable area can not be calculated straightforwardly. To calculate the DL success rate, using some geometry derivations, we can have four cases, defined by α, the angle between two intersecting points with respect to C_{JD}, β_D and the jammer location regarding the FN. Denote the distance between C_{JD} and (x_0, y_0) as d_{JC}. By denoting $D = R_D + d_{JC}$, for $\beta_D \in (0, \infty)$, we have the probability of success for DL transmission derived as:

$$P_s^d = \frac{\text{Viable downlink area}}{\text{Area of given circle } A_R}$$
$$= \begin{cases} \frac{A_R - A_{R_D}}{A_R} & D \leq R, \beta_D \neq 1 \\ \\ \frac{1}{A_R}\{A_R - A_{R_D} & D \in (R, R + 2R_D) \\ +S_{R_D} - \Delta_{R_D} & \beta_D \in (0,1) \quad \text{or} \\ +sign(\sin\alpha) & D \in (R, 2R_D - R) \\ \times(S_R - \Delta_R)\} & \beta_D > 1 \\ \\ \frac{1}{\pi}\arccos\frac{d_{FJ}}{2R} & d_{FJ} \in [0, R] \quad \text{and} \\ -\frac{d_{FJ}}{2\pi R}\sqrt{1 - \frac{d_{FJ}^2}{4R^2}} & \beta_D = 1 \\ \\ 0 & \text{others,} \end{cases} \tag{7}$$

where S_R and S_{R_D} denote the two circular sectors of FN and DL circle; Δ_R and Δ_{R_D} denote the triangle of two intersecting points and the centre of FN or DL circle; *sign*(*x*) is a function giving the sign of *x*. Note that when $\beta_D = 1$, the area is calculated as a circular segment defined using the middle point between jammer and the FN along with its perpendicular line's intersection points. The segment is the jammed area, which contains the jammer, and its size depends on the jammer location regards to the FN.

B. Uplink Transmission

In terms of UL, the leader will receive mixed signals from followers and the jammer. Note, as we justified in Section II that there is no multi-access interference among the followers by using CSMA or centralized radio resource allocation schemes. To detect the UL signal that carries voting message correctly, we assume that the SINR of the received signal at the leader satisfies

$$\text{SINR}_U = E[\frac{P_S|H_S(t)|^2}{d_F^\gamma}]/E[(\frac{P_J|H_J(t)|^2}{d_{FJ}^\gamma}+|N|^2)] \geq \beta_U, \tag{8}$$

where β_U is UL SINR detection threshold. Similarly, we can have

$$d_F^\gamma \leq \frac{P_S}{\beta_U(\frac{P_J}{d_{FJ}^\gamma} + \sigma^2)^{\frac{2}{\gamma}}}. \tag{9}$$

Therefore, we have the following circular boundary (C_{JU}, R_U) and its area A_{R_U}

$$(x - x_0)^2 + (y - y_0)^2 \leq R_U^2, \tag{10}$$

with its centre at

$$C_{JU} = (x_0, y_0), \tag{11}$$

and radius

$$R_U = \sqrt{(\frac{P_S}{\beta_U(\frac{P_J}{d_{FJ}^\gamma} + \sigma^2)})^{\frac{2}{\gamma}}}. \tag{12}$$

The circle is the bound of success and failure area, where the inner circle is viable, and the outer area is jammed, which is opposite of the DL case. Note that the interference and noise are integrated into the equation (12), and thus, it is compatible with any configurations. Given the fact that all voting nodes are evenly distributed in the area, the probability of success for UL transmission can be derived as:

$$P_s^u = \frac{\text{Viable UL area}}{\text{Area of the given circle}} = \begin{cases} \frac{A_{R_U}}{A_R} & R_U < R \\ 1 & R_U \geq R \end{cases} \tag{13}$$

Compared to the DL case, the UL case is straightforward as shown in equation (13), where given a weak jammer power plus noise power, the viable area can be larger than the considered consensus network (i.e., the circle of the radius R). In this case, all of the followers will have successful UL transmissions. For optimization, when the $R_U = R$, all nodes will have valid transactions, hence the optimal P_S can be worked out. Again, by considering the small fading factor, an instantaneous UL transmission may not meet the derivations in equations (12) and (13).

Given the equations (5), (11), and the leader's location C_0, we have the following property.

Remark 1: The centre points (x_0, y_0), centre of jamming DL area (x_D, y_D) and jammer location(x_1, y_1) are on a straight line.

The proof is straightforward since we have the following relationship: $\frac{y_c - y_0}{x_c - x_0} = \frac{y_1 - y_0}{x_1 - x_0}$. Since both circles' centers have the same gradient, hence they are on one straight line.

C. Probability of Successful Blockchain Transaction

In order to have a successful follower vote, both UL and DL must be successful between the follower and the leader. Thus, only the followers that meet both equations (4) and (10) will have a successful vote. According to the consensus principle of RAFT, only majority nodes (over 50%) success will have the transaction recorded in the blockchain. To calculate the probability of a successful transaction recognized by consensus network in RAFT based blockchain, according to (7) and (13), it is equivalent to calculate if the successful area (for both UL and DL) is more than half of the overall area. By writing as a formula,

$$P = p\Big(\frac{\text{Viable downlink area} \bigcap \text{Viable uplink area}}{\text{Area of given circle } A_R}\Big). \quad (14)$$

$\bigcap$ takes interaction area of two sets. In the next, we will derive the analytical expression of (14). It is worth mentioning that in RAFT protocol, the successful transmission happens when $P > 0.5$. It should be noted that the UL viable area can be overlapped with the DL jammed area. Here to make the analysis simple, we have assumed that UL and DL SINR threshold $\beta_D = \beta_U = \beta$. Depending on the value of β, we have the following theorem for different intersections of circles.

Theorem 1: For jammer located within the valid distance R and $\beta \in (0, \infty)$, we have the probability P of the successful transaction for the wireless RAFT blockchain networks as

$$P = \begin{cases} \frac{A_{R_U} - A_{R_D}}{A_R}, & \beta \in (0, \frac{1}{4}] \\ \frac{1}{A_R}\{A_R - A_{R_U} + S_{R_D} - \Delta_{R_D} & \beta \in (\frac{1}{4}, 1) \\ +sign(\sin\alpha_U)(S_{R_U} - \Delta_{R_U})\} & \bigcup(1, \infty) \\ \frac{A_{R_U}}{A_R}(\frac{2}{3} + \frac{\sqrt{3}}{4\pi}) & \beta = 1, \\ & A_{R_U} \in [0, A_R] \\ 0, & \text{others} \end{cases} \quad (15)$$

where S_{R_U} denotes the UL circle; Δ_{R_U} is the triangle of two intersecting points and the centre of UL circle; α_U denotes the angle between two intersecting points of the UL circle and DL circle with respect to the centre of DL circle.

Proof: By considering the cases of β, when $\beta \neq 1$, the success area is $A_{R_U} \cap \overline{A_{R_D}}$. For $\beta = 1$, the downlink area is divided into two circular segments, which are separated by the chord defined using the middle point between the jammer and FN, where the near side downlink segment to the jammer is the failed area A_{R_D}, hence the success area is again $A_{R_U} \cap \overline{A_{R_D}}$. ■

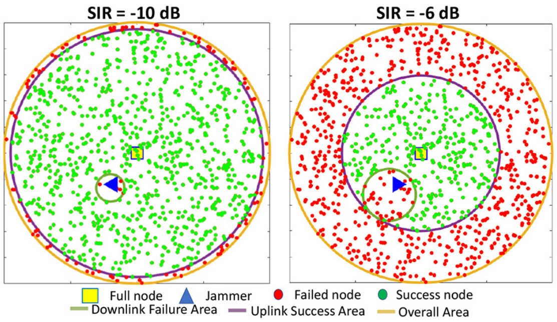

Fig. 2. Uplink and downlink transmission successful areas with two SINR threshold settings.

When β is small, taking $\beta = 0.1$ as an example, the maximum DL circle is always inside the UL circle, which makes the tangency of two circles the maximum jamming area. Due to the increasing β value, two circles start overlapping with each other, but the DL circle is always smaller than the half area of great circle R. The maximum area is reached at the maximum chord length for the DL circle.

Given equation (15), one can analytically calculate the success rate of the blockchain transaction in the wireless blockchain systems, where we can see that the probability of success depends on the β, jammer distance d_{FJ} and size of the circle A_R, hence it gives the relation of circle size with the power of the jammer and follower nodes. Note that the jammer can be placed in any location, including the region outside the circle, which naturally results in ineffective jamming. Unless the voter has a poor SINR value, such as 20dB, the jamming might be successful from a far distance. Thus, (15) provides an insightful guide to the indigenous wireless blockchain network design, parameter selections and optimizations.

It is worth mentioning the communication complexity of RAFT. Given RAFT consensus network with the number of n nodes and one of them is the leader. Hence, the vote message count for uplink and downlink will be $n - 1$ each side. Therefore, at least $2n - 2$ messages will be incurred during one consensus process. However, in practical deployment, the message will be attempted multiple times within the timeout frame, hence in the worst case, upon the retries t times, the system will confirm its final state. Therefore, the message quantity $f(n) = t(2n - 2)$.

IV. Simulation Results and Discussions

In order to validate the proposed wireless blockchain network models and derivations, a set of simulations are conducted. We assume the nodes are evenly distributed in a circle with radius $R = 100$ m with a fixed density (in total 1000 nodes, approximately 31847 nodes/km^2), the DL and UL SINR threshold maintains the same. We also assume that all nodes radiate the same level and omnidirectional signal. The jammer sends interference signals continuously at both UL and DL frequency bands.

A. Simulation 1: Uplink and Downlink Success Rates

The successful areas of UL and DL transmissions are shown in Fig. 2, where the successful nodes are marked in green, and failed ones are red. In this simulation, we assume $\gamma = 2.5$ and the detection SINR thresholds are $\beta = -10$ dB (left sub-figure) and $\beta = -6$ dB (right sub-figure), respectively. As to

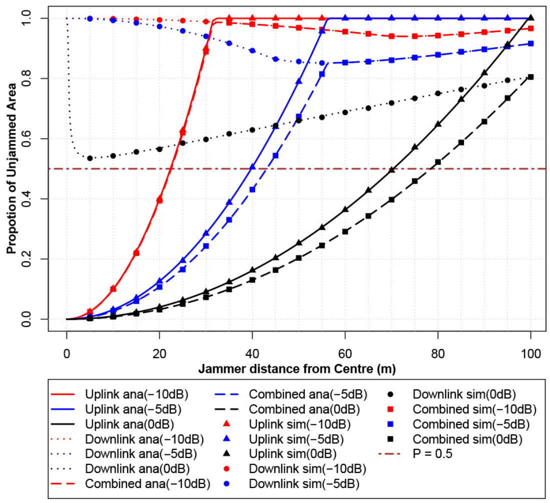

Fig. 3. Transaction success probability P vs. the jammer distance from origin (Analytical (ana), Simulation (sim)).

compare the influence of different SINR values, the location of the jammer is fixed at 30 m from the FN and maintains the same transmission power for both UL and DL.

Comparisons on two sub-figures in Fig. 2 gives a straightforward visual. When the required SINR threshold is high in the right-hand sub-figure (i.e., $\beta = -6$ dB), the consensus cannot be achieved since the number of failed nodes (in red) is more than the success ones (in green). However, with an increased receiver sensitivity (i.e., reduce the SINR threshold to -10 dB in this case), we can obliviously see that the successful blockchain consensus can be achieved since much more green nodes than red nodes.

B. Simulation 2: Success Rate vs. Jammer Location

This simulation shows the combined jamming area for different jammer location from the center of the FN. We have also shown the analytical result derived in equation (15) here for verification. It can be seen that in all cases, the analytical and simulation results match well in Fig. 3, where $\beta = -10$ dB matches the first part of equation (15), $\beta = -5$ dB matches second part and $\beta = 0$ dB matches third part.

Additionally, the plots shift to right while we increase the SINR threshold at the receiver. It verifies that the jammed area increases because of the increased SINR at the receiver, hence high SINR will lead to a higher failure rate. The trend for all three curves shows that the further jammer away from the center, the less jammed area it produces. Fig. 3 also shows the half area line, which indicates the jammer distance for a successful blockage and curves above the line denotes successful transaction and vice verse. When SINR $= -10$ and -5 dB, there is a plateau on the combined plot because of the complicated geometry shape of the overlapping circle with its moving center, and when SINR is small, the jammer is effective if it is close to the FN.

C. Simulation 3: Performance Analysis of Different SINRs

In this simulation, two cases of path loss exponential factors are considered, i.e., $\gamma = 2.5$ and 3.5. Fig. 4 shows the combined probability of half of the nodes successfully completing both UL and DL communication with FN. It can be seen that for both cases, the analytical and simulated results match well, which verifies the effectiveness of our derivations. The success rate reduces during the receiver SINR threshold increases because the sensitivity is not sufficient to distinguish the jammer among desired signals. Besides, there is a possibility that the jammer can be very close to the leader, hence resulting in failed UL / DL transmission even though receivers are rather sensitive (e.g., SINR $= -20$ dB). In addition, the success probability difference for $\gamma = 2.5$ and $\gamma = 3.5$ is insignificant when SINR is within large or small regions.

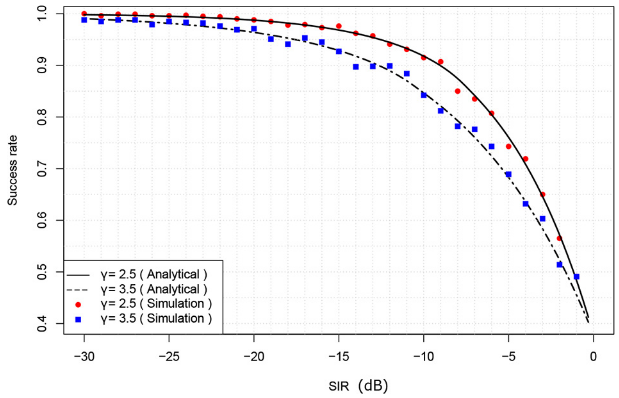

Fig. 4. Transaction success probability P with different SINR.

V. Conclusion

In this letter, we investigated the wireless blockchain networks for IoT systems based on RAFT, one of the most commonly used private chain consensus mechanisms. The security performance in terms of the transaction success rate has been analyzed by mapping it with the UL and DL wireless transmissions in the presence of a malicious jammer. Simulation results have been conducted to verify the effectiveness of derivations. Thus it provides a useful guide for the wireless blockchain system design, deployment, and optimization.

As for future work, the multiple-jammer case can be considered as an extension to make this letter more generic and practical. A predictive learning method is under development to solve the multi-jammer problem. The critical challenge in multi-jammer is the chaotic situation when the nodes' position in constant changing condition.

References

[1] B. Cao *et al.*, "When Internet of Things meets blockchain: Challenges in distributed consensus," *IEEE Netw.*, vol. 33, no. 6, pp. 133–139, Nov./Dec. 2019.

[2] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[3] P. Vasin. (2014). *BlackCoin's Proof-of-Stake Protocol v2 Pavel*. [Online]. Available: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[4] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.

[5] L. Lamport, "The part-time parliament," *ACM Trans. Comput. Syst.*, vol. 16, no. 2, pp. 133–169, May 1998.

[6] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *Proc. Annu. Tech. Conf.*, 2014, pp. 305–319.

[7] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proc. 3rd Symp. Oper. Syst. Design Implement. (OSDI)*. Berkeley, CA, USA, 1999, pp. 173–186.

[8] R. H. Deng, "Distributed systems," in *Computer Communications*, vol. 18, no. 1, 2nd ed. Amsterdam, The Netherlands: Elsevier, 1995, pp. 58–59, doi: 10.1016/0140-3664(95)90078-0.

[9] 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 J.*, vol. 6, no. 3, pp. 5791–5802, Jun. 2019.

[10] B. Leiding and W. V. Vorobev, "Enabling the vehicle economy using a blockchain-based value transaction layer protocol for vehicular ad-hoc networks," in *Proc. Mediterr. Conf. Inf. Syst.*, 2018, pp. 1–31.