On the Viable Area of Wireless Practical Byzantine Fault Tolerance (PBFT) Blockchain Networks

Oluwakayode Onireti, Lei Zhang and Muhammad Ali Imran
School of Engineering
University of Glasgow, Glasgow, G12 8QQ, UK
{Oluwakayode.Onireti, Lei.Zhang and Muhammad.Imran}@glasgow.ac.uk

***Abstract*—Distributed systems are crucial to the full realization of the Internet of Thing (IoT) ecosystem as it mitigates the challenges of trust, security, and scalability associated with the traditional centralized approach. In this paper, we present an analytical modeling framework for Practical Byzantine Fault Tolerance (PBFT)—a consensus method for blockchain in IoT networks. We define the viable area for the wireless PBFT networks which guarantees the minimum number of replica nodes required for achieving the protocol's safety and liveliness. We also present an analytical framework for obtaining the viable area which we later utilize for power optimization. Results show that significant energy saving can be achieved with the utilization of the viable area concept in wireless PBFT networks. The proposed framework can serve as a theoretical guidance for practical PBFT based wireless blockchain network deployment.**

I. Introduction

The advent of 5G technology and the autonomous deployment of billions of Internet of Things (IoT) devices present some fundamental design challenges in terms of security, slow operation, confidentiality, scalability, and high cost when third-party authentications are required [1], [2]. A fully autonomous IoT network can be achieved when different IoT devices (generally referred to as 'nodes') communicate in a distributed manner [3]. However, this requires a consensus method (CM) whereby nodes can agree on the validity of the communicated data. Meanwhile, as an underlying technology for cryptocurrencies, blockchain is a promising technology for addressing trust and security concerns, as well as high maintenance cost associated with IoT networks [4], [5]. Blockchain system relies on the consensus approach for agreeing on a new data hence, consensus methods used in blockchain can as well be applied to IoT networks. However, most IoT devices are battery powered and limited in bandwidth resources, communication and computational capabilities.

Practical Byzantine Fault Tolerance (PBFT)—a blockchain consensus method —is well suited for IoT as it offers low computational power and complexity. PBFT is a practical and improved protocol on BFT that was proposed in [6] and it achieves an order of magnitude improvement in response time over BFT by working in an asynchronous environment [7]. PBFT also achieves a reduction in the complexity level of messages from the exponential level associated with BFT to a polynomial level complexity [8]. PBFT offers significant reduction in energy consumption when compared with other blockchain CMs such as proof of work (PoW) and proof of stake (PoS) [9]. It is also not affected by the centralization and the "nothing at stake" problems associated with PoS. The PBFT protocol provides safety and liveliness when no more than $\lfloor \frac{n-1}{3} \rfloor$ out of the total n replica nodes are faulty [6]. This implies that neither operator or software errors nor adversary alterations can cause crash or adverse effect on the system if the number of faulty nodes is lower than this threshold. The PBFT wireless network is made up of IoT devices or nodes. When the header node in the PBFT network receives the client-IoT request, it starts the three phases of the PBFT consensus network namely, pre-prepare, prepare and commit [6]. In the pre-prepare, the header node multicast a pre-prepare message to other nodes (generally referred to as replica nodes) in the PBFT network while nodes communicate with each other in the prepare and commit phases. Transactions are then recorded on the blockchain after consensus is reached in the PBFT consensus network.

In this paper, we propose a novel framework for implementing the PBFT algorithm over a wireless channel. In particular, we consider that communications between the IoT nodes in the pre-prepare, prepare and commit phases are done over the wireless channel. We introduce the concept of viable area for a given view[1] and f number of faulty nodes noting that: 1) the conventional PBFT network requires at least $3f + 1$ replica nodes; 2) communications in the prepare and commit phases also require a specified minimum number of matching messages from other different replica nodes; and 3) replica nodes must be able to receive from a specified minimum number of other replica nodes. The viable area relates to the minimum coverage area that meets all the constraints required for a successful PBFT implementation. The viable area is decided by parameters such as the number of faulty replica nodes f, number of replica nodes in the network n, header/replica node transmit power and receiver sensitivity, and the pathloss components. As such, the viable area can provide a guide in practical deployment of blockchain systems by specifying how big the network should be. The main contributions of this work are summarized as follows

- We present an analytical framework for the viable area of

[1]The view change is used when the header node becomes faulty or breaks down. It allows other nodes in the PBFT network to select a new header.

978-1-7281-0962-6/19/$31.00 ©2019 IEEE

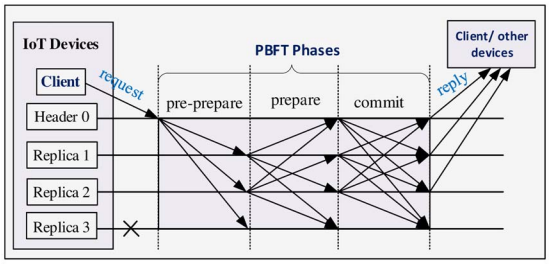

Fig. 1: Normal case operation of the Practical Byzantine Fault Tolerance (PBFT) network [6].

wireless PBFT networks. Our framework provides a link between the nodes (header and replicas) transmit power and receiver sensitivity, the PBFT network's coverage and the number of faulty nodes allowed for its successful operation. The proposed framework allows for the optimization of the network parameters such as the broadcast transmit power, receiver sensitivity, and coverage range.

- Noting that the nodes are battery driven IoT devices, we optimize the header/replica nodes broadcast transmit power for the scenario where the header node is located at the origin, which we later generalize to the case where the header is randomly located within the PBFT network.
- Furthermore, towards energy savings, we utilize the framework to determine the minimum transmit power required by replica nodes when responding to the client.

We first discuss the system model and assumptions in Section II, which include an overview of the normal PBFT and some assumptions in relation to the implementation of wireless PBFT. Using the system model for wireless PBFT in Section III, we introduce and define the viable area for the wireless PBFT networks. We present the numerical results in Section IV, while conclusions are drawn in Section V.

II. System Model and Assumptions

In this section, we present an overview of the conventional PBFT algorithm and discuss its implementation over a wireless network. We also present the system model and assumptions.

A. Practical Byzantine Fault Tolerance (PBFT)

The conventional PBFT network is made up of n replica nodes and it can tolerate a maximum of f faulty replica nodes. The relationship between n and f is defined from [6] as follows

$$f \leq \left\lfloor \frac{n-1}{3} \right\rfloor \tag{1}$$

In other words, the algorithm provides liveliness and safety as long as not more than $\lfloor \frac{n-1}{3} \rfloor$ replica nodes are faulty. The network will move through various views as it progresses and for each view, it selects one of the nodes as the header node. The nodes can take turns to be the header node. The header for the view v is denoted by v_p and can be obtained as follows

$$v_p = v \pmod{n} \tag{2}$$

We represent the set of replicas in a view by $\mathcal{S}$ and identify each replica by utilizing an integer in $\{0, 1, \ldots, |\mathcal{S}|-1\}$. Note that there could be more than $3f+1$ replica nodes, however, the additional replica degrades performance due to the increase in the amount of messaging without an improvement in the level of resilience. The operational steps of the conventional PBFT, which is illustrated in Fig. 1, are as follows

- The client sends a service request to the header node of the PBFT network.
- The PBFT network goes through three phases namely, the pre-prepare, prepare and commit[2].
- The client waits for $f+1$ replies from different replica nodes with the same response.

A client is an IoT device that makes a transaction or exchange information/record with other IoT devices referred to as replica nodes. The transaction are then recorded on the blockchain once consensus is reached in the consensus network.

B. Wireless PBFT Network Assumptions

In the first phase of the conventional PBFT network, the header node of the current view v broadcast a pre-prepare message to the whole network. We consider that n replica nodes are uniformly distributed in a circular PBFT network area with radius R such that the density of the replica nodes $\lambda = \frac{n}{\pi R^2}$. Furthermore, we consider a noise-limited wireless network with all replica nodes having equal receiver sensitivity β_1. Hence, the coverage range of the header node based on the maximum long-term averaged channel power, i.e., the effect of fading is averaged out, can be expressed from [10] as

$$R_1 = d_0 \left[\frac{P_1 K}{\beta_1} \right]^{\frac{1}{\gamma}}, \tag{3}$$

where P_1 is the transmit power of the header node. The parameter K is a unit-less constant that depends on the antenna characteristics and the average channel attenuation, d_0 is a reference distance for the antenna far field, and γ is the pathloss exponent. All replica nodes within the header node's coverage radius R_1 will receive the broadcasted pre-prepare message by the header and perform the necessary verification to ascertain the validity of the block.

Constraint 1: Given that there are f faulty nodes in the PBFT network, the number of replica nodes $\overline{n}$ within the coverage of the header node must satisfy the expression in (1). We define the coverage area of the header node within the network's coverage as $\mathcal{A}_1$. Hence, given the uniform distribution of the node, the constraint can be expressed as follows

$$\begin{aligned} \mathcal{A}_1 \lambda &\geq \overline{n} \\ &\geq 3f+1 \end{aligned} \tag{4}$$

Each replica node moves to the prepare stage once it accepts the pre-prepare, as illustrated in Fig. 1. In the prepare phase, the replica node broadcast a prepare message to the rest of the network and this include itself. Given the broadcast

[2]Here we focus on the wireless communication aspect. Details of the content of the messages, clock, time and ordering in each of the phases can be found in [6].

transmission power for each replica node P_2, the coverage range of each replica node can be expressed as

$$R_2 = d_0 \left[\frac{P_2 K}{\beta_1} \right]^{\frac{1}{\gamma}} \tag{5}$$

Note that we assume the same receiver sensitivity for the reception from the header and replica nodes' broadcast. To move to the next phase, each replica node must wait until it has $2f$ prepares from different replicas that match with the pre-prepare message.

Constraint 2: Given f faulty replica nodes in the PBFT network, for a non-faulty replica node to move out of the prepare state, it must be able to receive $2f$ prepare messages. Further, given that a node receives its own prepare message as well, a non-faulty replica node must receive the broadcast message of at least $2f-1$ other replica nodes. Thus, given that all replica nodes have the same transmit power and receiver sensitivity, the coverage area of a non-faulty replica node $\mathcal{A}_2$ jointly within the network and header node's coverage must be such that

$$\mathcal{A}_2 \lambda \geq 2f - 1 \tag{6}$$

Once the replica node has accepted the required $2f$ matching prepare messages it proceeds to the commit phase, as illustrated in Fig. 1. Similar to the prepare phase, the replica node broadcast a commit message to the whole network including itself. Further, each replica waits for $2f+1$ matching commit messages from different replica nodes. We note that 1) the header node is a non-faulty node since a faulty header will warrant a change of view (i.e., selection of a new header node), 2) each replica node receives the commit message from the header node, and 3) each replica node receives its own commit message. Hence, *constraint 2* also holds since each replica node must be able to receive commit message from effectively $(2f+1)-(1+1) = 2f-1$ other replicas in order to move to the next phase (i.e., reply).

Lastly, consensus is reached once the client (IoT node) has received at least $f+1$ replies from different nodes; this is the result of the PBFT consensus method and the transaction is recorded on the blockchain.

III. Viable Area of Wireless PBFT

The operation of wireless PBFT is limited by the coverage area of the replica nodes. In particular, we here consider that the coverage area of the header node in each view is determined by its transmit power and the replica nodes' receiver sensitivity denoted by P_1 and β_1, respectively. Since replica nodes must also broadcast and receive messages as well, their coverage is bounded by their broadcast transmit power and nodes (header and other replica nodes) receiver sensitivity, i.e., P_2 and β_1. We can thus define the viable area in a wireless PBFT network with n nodes, as the minimal area (equivalently, the minimum number of nodes) that meets the PBFT constraints listed in Section II-B. The viable area ensures that the minimum number of nodes are activated in each view of the wireless PBFT network, thus leading to significant energy savings and performance improvement.

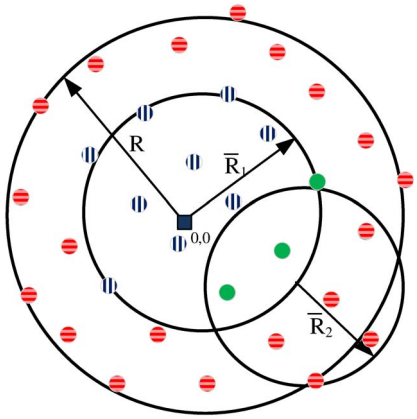

Fig. 2: Viable area of PBFT network with the header located at the origin.

Moreover, the viable area for a given number of faulty nodes specifies that transaction will be successful as long as f is not exceeded, and thus, it can be used in blockchain system design. In this section, we first define the viable area for the simplified case where the header node of a view is located at the center of the PBFT network's coverage area with radius R. We later extend this to the case where the header node is randomly located within the network's coverage area.

A. Header Node Located at the Origin

The viable area in a wireless PBFT network must satisfy *constraints 1 and 2* defined earlier. Hence, given that the header node is located at the origin, there exists a viable area with radius $\overline{R}_1$ such that at least $\overline{n} = 3f + 1$ replica nodes are within the area. Furthermore, a replica node located at the edge of the viable area must have at least $2f - 1$ replica nodes within its coverage which are jointly in the coverage of the header node. In Fig. 2, the header node is located at the origin (0,0)[3] and its coverage area R_1 is adjusted to $\overline{R}_1$ such that the average number of nodes in the coverage area $\pi\lambda\overline{R}_1^2 \geq \overline{n}$ (i.e., all green and vertically-stripped blue nodes). Furthermore, replica nodes located at a distance $\overline{R}_1$ from the header node must have an average of $2f - 1$ other replica nodes within its coverage which are jointly in the coverage of the header node (i.e. the green replica nodes). Note that all replicas located at a radial distance less than $\overline{R}_1$ will also meet this condition.

In order to obtain and define the viable area, we rely on the expressions in equations (3)-(6) and note the relationship between the coverage radius and the transmit power for a given fixed pathloss exponent and receiver sensitivity. We set the objective function on minimizing the sum of the broadcast transmit power of the header node and a typical replica node located at the edge of the viable area while satisfying all the defined constraints. The objective function is defined as follows

$$\underset{P_1, P_2}{\text{minimize}} \; P_1 + P_2 \tag{7}$$

[3]We define the origin as the centre point of the PBFT network coverage area

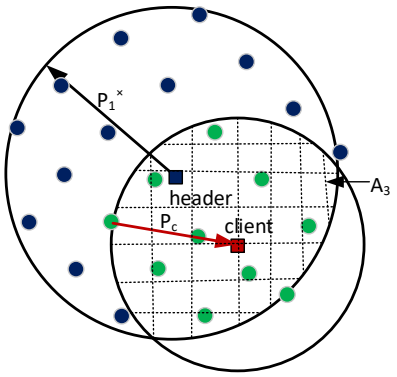

Fig. 3: Illustration of the minimum broadcast transmit power required by the replicas when responding to the client (IoT device).

Note that P_2 is the broadcast transmit power of a typical replica node on the edge of the viable area. From (3), (4) and the fact that $\mathcal{A}_1$ is a circular coverage area with radius $\overline{R}_1$, we can define the first constraint as follows

$$\lambda\pi\kappa P_1^{\frac{2}{\gamma}} > 3f+1 \tag{8}$$

where $\kappa = d_0^2\left(\frac{K}{\beta_1}\right)^{\frac{2}{\gamma}}$. Furthermore, noting that the area $\mathcal{A}_2$ required for the second constraint is the intersecting area based on selecting P_1 and P_2, we can define the coverage area that satisfies constraint 2 as follows

$$\kappa P_2^{\frac{2}{\gamma}}\sin^{-1}\left(\frac{y(P_1,P_2)}{\omega P_2^{\frac{1}{\gamma}}}\right)+\kappa P_1^{\frac{2}{\gamma}}\sin^{-1}\left(\frac{y(P_1,P_2)}{\omega P_1^{\frac{1}{\gamma}}}\right) \tag{9}$$
$$-y\left(P_1,P_2\right)\left(\frac{\omega P_2^{\frac{2}{\gamma}}}{2P_1^{\frac{1}{\gamma}}}+\sqrt{\kappa P_1^{\frac{2}{\gamma}}-\kappa P_2^{\frac{2}{\gamma}}+\frac{\kappa P_2^{\frac{4}{\gamma}}}{4P_1^{\frac{2}{\gamma}}}}\right) > 2f-1$$

where $\omega=\sqrt{\kappa}$, $y\left(P_1,P_2\right)=\sqrt{\kappa P_2^{\frac{2}{\gamma}}-\frac{\kappa P_2^{\frac{4}{\gamma}}}{4P_1^{\frac{2}{\gamma}}}}$.

Other constraints required for defining the viable area in wireless PBFT include limiting the transmit power of the header node and replica nodes. Here, we set the maximum transmit power of the header node $P_1^{\max}=\left(\frac{R}{\omega}\right)^{\gamma}$ to ensure that all replica nodes in the network's coverage area can be served by the header node when such is required. The replica node's maximum transmit power is a network defined parameter which is set to $P_2^{\max}=\alpha P_1^{\max}$, where $\alpha>1$. Hence, we set the following constraints

$$\begin{aligned} 0 \le P_1 \le P_1^{\max} \\ 0 \le P_2 \le P_2^{\max} \end{aligned} \tag{10}$$

Consequently, the optimization problem with the objective function defined in (7) and constraints defined in (8)-(10) can be solved by using a classic method such as the interior-point method [11], which is integrated into the "fmincon" Matlab function. We denote the optimization results as $P_1^{\star}$ and $P_2^{\star}$.

Constraint 3: The last phase of the PBFT network requires that the client must have at least $f+1$ response from the committed replica nodes. Hence, given that the number of replica nodes in the viable area is defined by the header's transmit power $P_1^{\star}$, we can define the minima area $\mathcal{A}_3$ (equivalently the minimum number of replicas) within the viable area required for successful implementation of the replicas response as

$$\mathcal{A}_3\lambda \ge f+1 \tag{11}$$

Here, we estimate the minimum transmit power for the replica nodes to satisfy this requirement given that all replica nodes transmit with the same power. Fig. 3 illustrates our approach for obtaining the minimum replica node transmit power P_c for achieving the client reply. The client could be located within or outside the coverage area of the PBFT network's coverage. As shown in Fig. 3, we define a circular area with radius R_c centered at the client node location such that its intersecting area with the viable coverage area (defined with the header node transmit power $P_1^{\star}$) is equivalent to $\mathcal{A}_3$. Given the client's receiver sensitivity β_2, we can obtain the minimum transmit power P_c from constraint 3 defined in (11) by transposing R_c and solving the expression below

$$-y(P_c)\left(\frac{\overline{\kappa}P_c^{\frac{2}{\gamma}}-a_1+d_1^2}{2d_1}+\sqrt{a_1-\overline{\kappa}P_c^{\frac{2}{\gamma}}+\left(\frac{\overline{\kappa}P_c^{\frac{2}{\gamma}}-a_1+d_1^2}{2d_1}\right)^2}\right)$$
$$+\overline{\kappa}P_c^{\frac{2}{\gamma}}\sin^{-1}\left(\frac{y\left(P_c\right)}{\overline{\omega}P_c^{\frac{1}{\gamma}}}\right)+a_1\sin^{-1}\left(\frac{y\left(P_c\right)}{\sqrt{a_1}}\right)=\frac{f+1}{\lambda} \tag{12}$$

where $\overline{\kappa}=d_0^2\left(\frac{K}{\beta_2}\right)^{\frac{2}{\gamma}}$, $\overline{\omega}=\sqrt{\overline{\kappa}}$, $a_1=\overline{\kappa}P_1^{\star\frac{2}{\gamma}}$, $y\left(P_c\right)=\sqrt{\overline{\kappa}P_c^{\frac{2}{\gamma}}-\left(\frac{\overline{\kappa}P_c^{\frac{2}{\gamma}}-a_1+d_1^2}{2d_1}\right)^2}$, d_1 is the distance between the client and the header node. The minimum replica node transmit power for successful reply to the client can be obtained from (12) with the use of a linear search method such as the Newton–Raphson method.

B. Header displaced from the origin

The case where the header node is displaced from the origin is illustrated in Fig. 4. In this scenario, the viable area must as well meet the conditions defined in constraints 1 and 2. As illustrated in Fig. 4, there exists a viable area that is defined based on the intersection of the coverage area of the header node and the PBFT network coverage area. The viable area is defined by adjusting the header's coverage radius $\overline{R}_1$ such that its intersecting area with the PBFT coverage is such that the number of replica nodes within the area exceeds $\overline{n}$ (all green and vertically-stripped blue nodes). Furthermore, the header node on the edge of the viable area must always satisfy constraint 2, i.e., $\mathcal{A}_2\lambda > 2f-1$. It can be shown mathematically that the minimum of $\mathcal{A}_2$ over the viable area is achieved at the two intersecting points of the PBFT and the header nodes coverage if such exists, i.e., h_1 and h_2. Otherwise, the solution defined for the case with the header node located at the origin holds. In the following, we define the optimization function required for defining the viable area

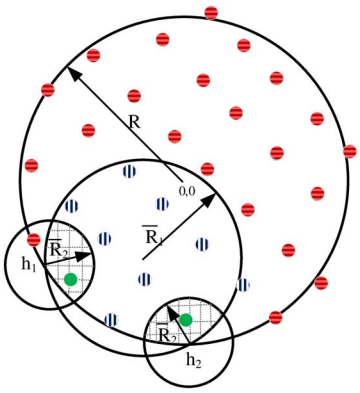

Fig. 4: Viable area of PBFT network with randomly located header node.

when the header node is not located at the origin. The objective function is as defined in (7). From (3), (4) and the fact the PBFT network nodes are uniformly distributed in a circular area with radius R, we can define the header node radius $\overline{R}_1$ that satisfy the first constraint as follows

$$-y(P_1)\left(\frac{a_2-\kappa P_1^{\frac{2}{\gamma}}}{2d_1}+\sqrt{\kappa P_1^{\frac{2}{\gamma}}-R^2+\left(\frac{a_2-\kappa P_1^{\frac{2}{\gamma}}}{2d_1}\right)^2}\right)$$
$$+R^2\sin^{-1}\left(\frac{y\left(P_1\right)}{R}\right)+\kappa P_1^{\frac{2}{\gamma}}\sin^{-1}\left(\frac{y\left(P_1\right)}{\omega P_1^{\frac{1}{\gamma}}}\right)>3f+1 \tag{13}$$

where $y(P_1)=\sqrt{R^2-\left(\frac{a_2-\kappa P_1^{\frac{2}{\gamma}}}{2d_1}\right)^2}$, $a_2=R^2+d_1^2$, d_2 is the distance between the view's header node and the origin. Furthermore, the area $\mathcal{A}_2$ for satisfying the second constraint is based on selecting P_1 and P_2 such that the number of replica nodes in each of the shaded portions in Fig. 4 exceeds $2f-1$. Note that points h_1 and h_2 are identical in terms of the area of the shaded portion attained. In addition, moving in any direction from either point leads to an increase in the coverage overlap area of a replica node located on the edge of the viable area. Hence, any replica node that is located on the edge of the viable area will satisfy the second constraint. The shaded area has a shape referred to as the circular triangle whose closed-form expression is given in [12]. We thus define the area as a function of the header and replica node's transmit power in (14) shown on the top of the next page. Similar to the case with the header located at the origin, the optimization can also be solved by using the "fmincon" Matlab function.

In addition to power optimization, the expressions in (7)-(9) and (13)-(14) can be used to check if we can have a successful transaction with wireless PBFT network and also in the designing the network (e.g. determining the coverage range of the consensus network, i.e., R).

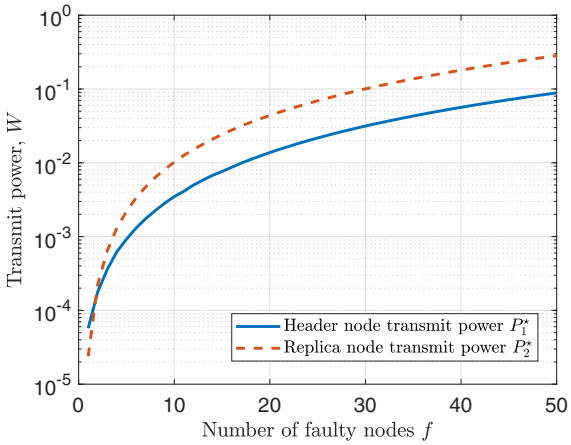

Fig. 5: Effect of the number of faulty nodes on the header and replica nodes transmit power, $\lambda=\frac{1}{\pi 1000}$ nodes/m^2.

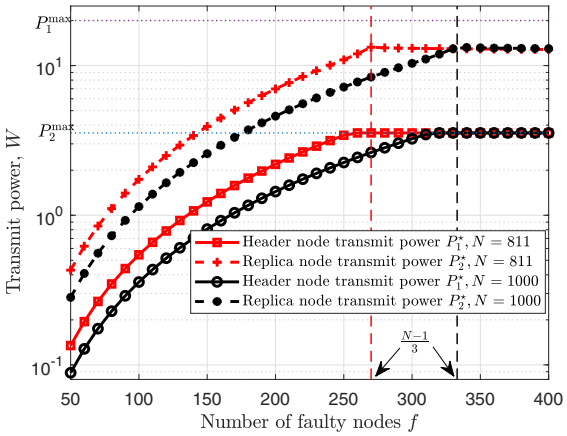

Fig. 6: Effect of the number of faulty nodes on the header and replica nodes transmit power, $\lambda=\frac{N}{\pi 1000^2}$ nodes/m^2, $N=811,1000$.

IV. Numerical Results

In this section, we present some numerical results to illustrate our analytical findings. The system parameters are as follows: $K=1, d_0=1, \beta_1=-84.5$ dBm, $\beta_2=-84.5$ dBm, $\gamma=4$ and $\alpha=10$. Furthermore, replica nodes are uniformly distributed within the wireless PBFT networks circular coverage area with density $\lambda=\frac{1}{\pi 1000}$nodes/m^2. We set the PBFT coverage radius $R=1000$ m and show results for the case where the header is located at the origin.

In Figs. 5 and 6, we plot the header's broadcast transmit power $P_1^\star$, which corresponds to the viable area with radius $\overline{R}_1$, for a varying number of faulty replica nodes f. The broadcast transmit power $P_1^\star$ must be utilized by the header node in all the PBFT phases, i.e. pre-prepare, prepare and commit phases. Furthermore, we also plot the corresponding broadcast transmit power $P_2^\star$ of a replica node located on the edge of the viable area. The header node and replica nodes must transmit with at least $P_1^\star$ and $P_2^\star$, respectively, for a successful wireless PBFT operation. Utilizing $P_1^\star$ and $P_2^\star$ for the header node and replica nodes, respectively, ensures significant energy savings without sacrificing the reliability of

$$\frac{1}{4}\sqrt{(c_1+c_2+c_3)(c_2+c_3-c_1)(c_1+c_3-c_2)(c_1+c+2-c_3)}+\sum_{k=1}^{2}\left(\kappa P_k^{\frac{2}{\gamma}}\sin^{-1}\frac{c_k}{2\omega P_k^{\frac{1}{\gamma}}}-\frac{c_k}{4}\sqrt{4\kappa P_k^{\frac{2}{\gamma}}-c_k^2}\right)$$
$$+R^2\sin^{-1}\frac{c_3}{2R}-\frac{c_3}{4}\sqrt{4R^2-c_3^2}>2f-1 \qquad (14)$$

where $c_i(P_1,P_2)\ \forall i\in 1,2,3$ are the three cord lengths of the circular triangle defined in [12] for a fixed PBFT network with replica nodes distributed in a circular area with radius R.

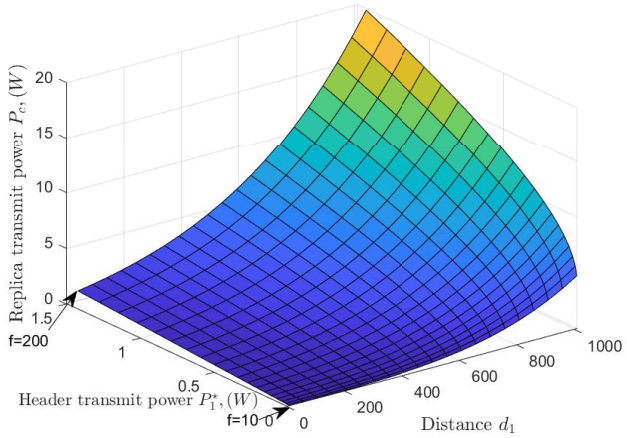

Fig. 7: Effect of the number of faulty nodes on the replica transmit power during the reply phase, $\lambda=\frac{1}{\pi 1000}$ nodes/m^2.

the PBFT network. It can be seen from Figs. 5 and 6 that increasing the number of faulty nodes leads to an increase in the replica and header nodes transmit power. This is because the number of nodes in the coverage of the header and replica nodes must increase in order to guarantee the safety and liveliness of the PBFT network and hence the increased transmit power. Moreover, increasing the number of replica nodes for a fixed number of faulty nodes f leads to a reduction in the transmit power of both the header and replica nodes as long as $N>3f+1$. Fig. 6 further shows that the transmit powers of the header and replica nodes are bounded by either the maximum transmit power ($P_1^{\max}$ or $P_2^{\max}$) or the number of faulty nodes reaching $\frac{N-1}{3}$.

In Fig. 7, we plot the minimum transmit power P_c required by the replica nodes to send their reply message to a client located at a distance d_1 away from the header node. It can be seen that increasing the number of faulty nodes leads to an increase in transmit power required by the replica nodes for sending the reply message to the client. Moreover, the transmit power far exceeds the broadcast transmit power used by the replica nodes during the pre-prepare, prepare and commit phases of the wireless PBFT network.

V. Conclusions

In this paper, we investigated the performance of the Practical Byzantine Fault Tolerance (PBFT) protocol when implemented over the wireless network. We first reviewed the normal PBFT protocol and presented its framework over the wireless channel while taking the protocols implementation constraints into consideration. Then we define the viable area of the wireless PBFT networks in terms of the number of faulty replica nodes f, number of replica nodes in the network n, header/replica node transmit power and receiver sensitivity, and the pathloss components. The viable area achieves liveliness and safety for the wireless PBFT network with the minimum number of replicas and minimum broadcast transmit power and thus results in significant energy savings. As an application of the viable area of wireless PBFT, we analyzed the minimum replica node transmit power required to achieve a successful response to the IoT client. Numerical results show that contrarily to the normal PBFT whose performance is bounded by $3f+1$, the wireless PBFT is further bounded by the maximum broadcast transmit power.

Acknowledgement

The work was supported by U.K. Engineering and Physical Sciences Research Council under Grant EP/S02647X/01.

References

[1] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *Proc. IEEE/ACM Int. Conf. Computer-Aided Design (ICCAD)*, Nov. 2014, pp. 417–423.

[2] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of internet of things (IoT)," *International Journal of Computer Applications*, vol. 111, no. 7, 2015.

[3] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[4] 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.

[5] 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*, 2019.

[6] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Third Symposium on Operating Systems Design and Implementation*, New Orleans, USA, Feb. 1999.

[7] N. Chondros, K. Kokordelis, and M. Roussopoulos, "On the practicality of practical byzantine fault tolerance," in *Middleware 2012*. Springer, Jan. 2012, vol. 7662, pp. 436–455.

[8] L. Zhang and Q. Li, "Research on consensus efficiency based on practical byzantine fault tolerance," in *Proc. Identification and Control (ICMIC) 2018 10th Int. Conf. Modelling*, Jul. 2018, pp. 1–6.

[9] Z. Zibin, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web and Grid Services*, 2017.

[10] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[11] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[12] M. Fewell, "Area of common overlap of three circles," Australian Maritime Operations Division Defence Science and Technology Organisation, Tech. Rep. DSTO-TN-0722, 2006.