Wireless PBFT Consensus Blockchain Networks

Ziyi Zhou

Submitted in fulfilment of the requirements for the
Degree of Doctor of Philosophy

School of Engineering
College of Science and Engineering
University of Glasgow

August 2024

Abstract

As wireless networks evolve towards increasingly heterogeneous environments with a growing number of mobile users, ensuring security and privacy becomes paramount. Blockchain technology, renowned for its decentralization and security features, presents a promising solution to these challenges. Practical Byzantine Fault Tolerant (PBFT), a voting-based consensus blockchain, is suitable for the wireless network because it is not computationally intensive, as most mobile devices are computationally limited due to the battery size and processing limitations. Moreover, PBFT can provide the essential byzantine fault tolerance to provide resistance to network failure and malicious attacks. This thesis investigates the application of PBFT consensus mechanisms to wireless networks, specifically focusing on IEEE 802.11 protocols, base station-enabled architectures and a hybrid network solution.

The performance of the wireless PBFT network using the IEEE 802.11 broadcast scheme under unsaturated conditions is investigated. Through a Markov model, the throughput, transmission success probability, and transaction confirmation delay of such a network are derived. View change is a mechanism incorporated to provide liveness to the PBFT, but frequent view change can undermine the overall performance of the PBFT network by delaying the consensus. The view change delay is introduced and derived in reference to the transaction confirmation delay. The impacts of channel contention from the non-PBFT nodes on the performance of the wireless PBFT network are further investigated. Channel contention impairs the transmission success probability and increases the chance of view change. The findings highlight a critical minimum transmission success probability required for effective PBFT consensus, proposing optimal configurations of the packet arrival rate and contention window size to balance success probability and network performance.

Furthermore, this thesis proposes an innovative PBFT framework leveraging base stations for inter-node communication. This approach reduces communication

complexity and node transmit power while enhancing scalability and consensus success probability. The uplink and downlink communication between the base station and nodes are modelled based on the signal-to-interference-plus-noise ratio (SINR) threshold, which measures the strength of the wanted signal compared to the unwanted interference and noise. A good SINR is essential for reliable data transmission speed and integrity. A novel 'timeout' mechanism is incorporated to mitigate communication overheads. The performance is evaluated by metrics including consensus success probability, communication complexity, view change delay, view change occurrence probability, average transmit power, consensus delay and consensus throughput. The proposed framework demonstrates improvements in consensus success probability and throughput and reduced consensus delays compared to traditional PBFT implementations. A special case with f deterministic Byzantine nodes is also presented. The optimal configuration for achieving the target consensus success probability to provide analytical guidance for deploying wireless PBFT networks is analysed and demonstrated with numerical results.

To mitigate the influence of the poor wireless connection, which results in increased view changes and reduced consensus success probability, a hybrid PBFT network integrating a private and a public cloud is introduced. The security performance of the hybrid network is assessed in the presence of crashes and malicious attacks with decentralised and centralised coordination modes. This hybrid approach shows enhanced security capabilities compared to conventional PBFT, particularly when the private cloud is secure.

Overall, this thesis provides a comprehensive analysis of PBFT's application in wireless networks, offering practical insights and solutions to improve security, efficiency, and scalability in future wireless and IoT environments.

University of Glasgow

College of Science & Engineering

Statement of Originality

Name: Ziyi Zhou

Registration Number: XXXXXXX

I certify that the thesis presented here for examination for a PhD degree of the University of Glasgow is solely my own work other than where I have clearly indicated that it is the work of others (in which case the extent of any work carried out jointly by me and any other person is clearly identified in it) and that the thesis has not been edited by a third party beyond what is permitted by the University's PGR Code of Practice.

I declare that the thesis does not include work forming part of a thesis presented successfully for another degree.

I declare that this thesis has been produced in accordance with the University of Glasgow's Code of Good Practice in Research.

I acknowledge that if any issues are raised regarding good research practice based on review of the thesis, the examination may be postponed pending the outcome of any investigation of the issues.

Signature: .....

Date: .....

Contents

List of Tables

List of Figures

List of Acronyms

- `MEC` - multiple edge computing
- `DDoS` - distributed denial of service
- `P2P` - peer-to-peer
- `THz` - terahertz
- `mmWave` - millimeter wave
- `IoT` - Internet of Things
- `PoW` - proof of work
- `PBFT` - practical byzantine fault tolerance
- `DPoS` - delegated proof of stake
- `LPoS` - leasing proof of stake
- `PoB` - proof of burn
- `PoI` - proof of importance
- `PoC` - proof of capacity
- `RPCs` - remote procedure calls
- `DAG` - direct acyclic graph
- `XRP` - Ripple
- `RTS` - request to send
- `CTS` - clear to send
- `UL` - uplink
- `DL` - downlink

- `MSE` - Mean Square Error
- `BER` - Bit Error Rate
- `SINR` - signal-to-noise-plus-interference ratio
- `BS` - base station
- `WBNs` - wireless blockchain networks
- `CT` - channel contention
- `ACK` - acknowledgment
- `CDF` - cumulative distribution function
- `SBS` - single base station
- `PPP` - Poisson point process
- `MBS` - multiple base stations
- `OMA` - orthogonal multiple access
- `PDF` - probability density function
- `CCDF` - complementary cumulative distribution function
- `SNR` - signal-to-noise ratio

Acknowledgements

I would like to express my deepest gratitude to my supervisor, Dr. Oluwakayode Onireti, who has been an invaluable mentor since the beginning of my academic career. His dedication, persistence, attentiveness, and enthusiasm have greatly inspired and influenced my research, which I believe will enlighten me throughout my life. It has been a remarkable journey as a PhD student under his guidance.

Moreover, I would like to thank my second supervisor, Prof Lei Zhang, who also helped me both academically and in daily life.

I would also like to thank my friends, especially my girlfriend, for their companionship during my PhD period. I could not have reached this point without the inspiration sparked by our shared wisdom and discussions.

Finally, I would like to thank my family for their financial and mental support, which are crucial for my PhD journey.

Chapter 1

Introduction

1.1 Overview

With the rapid development of communication techniques, mobile users and devices have increased significantly in the past few years. According to IBM [1], the number of connected devices in 2020 was over 25 billion and is forecasted to surpass 100 billion by 2050. The global mobile traffic volume was 7.462 EB/month in 2010, and this traffic is predicted to be 5016 EB/month in 2030 [2]. The continuous evolution and pervasive integration of mobile applications into everyday life have transformed the majority of the global population into mobile users. The wireless network plays a significant role in human life. However, the ever-increasing number of connected devices (like PCs, smartwatches, wearable health sensors, and even connected vehicles) will use tremendous wireless spectrum resources and pose a significant challenge to wireless network operators. The current network is centralised, where all users and devices are connected to cloud centres, allocating spectrum resources, storing data from connected devices as a database, and exchanging information with other centres. At present, this centralised network structure provides relatively reliable service for users. However, in the foreseeable future, the network will be more dynamic, heterogeneous, and massive. The number of mobile users is expected to grow explosively like now in the future. Meanwhile, state-of-the-art cloud centres are not scalable and intelligent enough [3]. They require tremendous computational and storage resources, and this expansion rate is not comparable to users' growth [4].

Other problems that are aroused by the centralised wireless network include data security, privacy, and caching constraints. In the centralised framework,

users' data is managed and stored by several cloud data centres, which are vulnerable to hackers' attacks and cloud centres' malfunction. This will greatly threaten the integrity, security and privacy of users' data. Furthermore, privacy in mobile networks is becoming more and more critical with the emergence of novel applications such as Industry 4.0 [5], automated vehicles [6], and medical applications [7,8], where even a minor failure can lead to disastrous consequences. Besides, due to the explosion of wireless network users, the tremendous demand for mobile users will pose a serious storage problem for the network operators under a centralised scheme [9]. Moreover, the upcoming 6G network has enlightened a set of more data-intensive and low-latency applications [10], which poses more challenges to the current wireless networks. The next-generation network is expected to provide ultra-high throughput, high reliability, low latency, high connectivity, and ubiquitous coverage to satisfy the needs of heterogeneous nodes and infrastructures [11].

The challenges faced by the wireless networks can be summarised as

- **Scalability:** The exponential growth in the number of connected devices strains network resources and management capabilities [12].
- **Security:** Centralised wireless networks are inherently vulnerable to various security threats, including unauthorized access, data breaches, and denial-of-service attacks [13, 14].
- **Decentralization:** Traditional wireless networks rely heavily on centralised architectures, which can create bottlenecks, single points of failure, and inefficiencies [15].
- **Interoperability:** Ensuring seamless communication between diverse devices and networks remains a complex task, often hindered by proprietary technologies and standards [16].

The advent of blockchain [17] technology has posed a plausible solution to the next-generation network. Blockchain has been applied in various areas, and the most famous application is Bitcoin [18], a cryptocurrency that has been successfully running for over 10 years. In addition to cryptocurrency, blockchain has displayed promising potential in recruitment and human management [19,20], cybersecurity [21, 22], energy coordination [23, 24], payment system [25, 26], transportation [27], the IoT [28], and finance [29]. Blockchain is a distributed ledger operated in a P2P manner that does not require supervision from a third party [30]. This attribute guarantees the stability of the network operation,

privacy, and security of users' data since each participant in the wireless blockchain network possesses a complete backup of the ledger and possesses the authority to append new blocks to the ledger. The transaction between nodes will be recorded on the block and broadcast to the entire network using the cryptographic principle. Once a block is added, it can not be modified anymore. Each node in this network validates the transaction and user's status by a consensus algorithm [31]. All recorded information/transactions in the blockchain are verified by all the peers and are thus immutable. Hence, using blockchain, the next-generation network can permanently record all events with its corresponding time frame [32]. Thus, this prevents the entire network from paralysing. Even if some nodes are compromised, they can recover and return to normal operation by downloading the ledger from their peers. In this regard, blockchain offers decentralisation to the next-generation network [33], reducing the reliance on centralised entities and improving the network's scalability. Other techniques, such as multiple edge computing (MEC) [34], could be a promising solution to problems brought by the centralised network for its eminent emphasis on performance optimization, real-time data processing and latency reduction. The future wireless network can benefit from the MEC in the following aspects

- **Latency-sensitive applications:** MEC enables applications like autonomous vehicles, and industrial IoT, where low-latency data processing is critical.
- **Scalability:** MEC fosters the scalability of IoT ecosystems by distributing computational workloads closer to the data source.

However, compared with MEC, blockchain can provide decentralised consensus among the network participants. Moreover, blockchain promotes node trust by enabling direct and secure interactions [35]. For example, private blockchain introduces identity management [36], which facilitates authorisations and authentication, and reduces the chances of malicious attacks. In addition, with the deployment of blockchain, the compromised nodes have a limited impact on the whole system. They can be quickly recovered by backing up from the neighbouring nodes, improving the resilience to attacks like distributed denial of service (DDoS) [10]. Therefore, blockchain is capable of improving the privacy and security of the next-generation network with enhanced immutability, resilience, transparency, provenance, immutability, distribution, and decentralization [37]. A recent use case has showcased the role of blockchain in the wireless network, which is the Helium network. It enables individuals to provide hotspots for IoT devices to enhance coverage and connectivity. Blockchain technology is used to

track and reward contributors with cryptocurrency based on the amount of data and coverage they provide.

Blockchain technology can also be of great advantage in securing, storing and managing data [18, 38, 39]. The next-generation network, composed of all kinds of devices (like smartphones, vehicles, smart grids, and base stations), generates large amounts of unstandardized data, which are difficult to collect, store, and utilize for network optimization [40]. The introduction of blockchain technology can handle this problem by setting up a platform that requires every participant to upload a uniform format of data. As a consequence, massive amounts of data can be used efficiently.

Even though the present blockchain is limited by scalability and storage issues, some new approaches, such as layer-2 solutions and rollups, are being developed to address those, which increase the feasibility of the deployment of the blockchain.

By leveraging blockchain, wireless networks can achieve enhanced security, greater scalability, improved decentralization, and better interoperability. Specifically, blockchain can provide

- **Enhanced Security:** Through cryptographic validation and consensus mechanisms, blockchain can secure communication and data exchange in wireless networks [41, 42].
- **Decentralised Network Management:** Blockchain enables decentralised management, reducing the reliance on central authorities and mitigating single points of failure [43, 44].
- **Interoperability:** Blockchain provides standardized protocols and interfaces, facilitating interoperability between different wireless networks and devices and simplifying the data exchange process [45, 46].
- **Automated Data Management:** Blockchain supports smart contracts that can automatically execute predefined rules and logic, simplifying data management processes, reducing human intervention, and increasing data management efficiency [47, 48].
- **Enhanced Trust:** Blockchain can securely log all transactions and interactions within the wireless network. Once a transaction is recorded, it cannot be altered or deleted. This ensures that any unauthorized activity can be traced back with certainty, improving the overall security and accountability of the network [49].

1.2 Original Contribution

The thesis aims to investigate the plausibility of deploying the blockchain technique using wireless networks, which can provide theoretical guidance for further industrial application. The thesis makes the following contributions:

1. **Performance analysis of PBFT-based wireless Networks with IEEE 802.11**

    - This thesis proposes a wireless Practical Byzantine Fault Tolerance (PBFT) network using the IEEE 802.11 broadcast scheme. The network is modelled with the transmission probability τ calculated through a state transition diagram. Based on the transmission success probability, the metrics of success probability, transaction confirmation delay, and throughput are further derived. The channel contention from the non-PBFT users is also taken into consideration, and how channel contention affects the performance of the wireless PBFT network is presented. A mathematical relationship between the PBFT success probability and transmission probability is provided. The proof and derivation of view change delay reveal the average view change delay under different network sizes in reference to the transaction confirmation delay. Moreover, we define the optimal transmission probability of IEEE 802.11 that maximizes the throughput of the network while not sacrificing the consensus success probability. The comprehensive and optimal pairs of its determining factors, contention window size, and packet arrival rate are both presented.

2. **Base Station-Enabled wireless PBFT network**

    - To improve the scalability of the wireless PBFT network, the research moves onto a novel framework for implementing PBFT in cellular networks. The uplink and downlink communications between the base stations and the PBFT nodes are analytically modelled, and their success probabilities are derived. The communication complexity of the consensus process of the PBFT is derived. Compared to the wireless PBFT network using IEEE 802.11, this framework outperforms with much lower communication complexity by introducing the *timeout* mechanism at the base stations. The proof and derivation of the view change occurrence and average view change delay are presented, highlighting the resiliency of the cellular PBFT network.

The simulation results prove that the consensus success probability can achieve 100%, even with a large-scale PBFT network. This indicates that incorporating the base station into the PBFT network can address the scalability restraint of the PBFT.

3. **Security analysis of a hybrid PBFT network with a cloud framework**

   - To mitigate the influence of the view change delay and consider a more practical scenario where crashes and malicious attacks can both exist in the wireless PBFT network, the research further moves onto the security of a hybrid PBFT network, which consists of a private and a public cloud. The impact of crash and malicious attacks on the security of the hybrid PBFT network is numerically analyzed and investigated under the centralised and decentralised coordination modes. The finding of a special case suggests that the secure private cloud can further enhance the security of the hybrid PBFT network.

1.2.1 Motivations

Several works have been done to explore the plausibility and feasibility of deploying blockchain to wireless networks or evaluating the performance of wireless blockchain networks. In this regard, prior research in [50] explored the minimal number of nodes required to ensure safety and liveness in a PBFT network. Luo [51, 52] investigated the performance of the PBFT implements on the 6G communications with terahertz (THz) and millimeter wave (mmWave), which is evaluated by the consensus success rate, latency, throughput, reliability gain, and energy consumption. A multi-layer PBFT consensus is proposed in [30]. Compared to the traditional PBFT, the proposed algorithm achieves much lower communication complexity, but the latency is greatly increased. In [53], a sharding scheme is incorporated in the PBFT to reduce energy consumption during the consensus process. PBFT nodes are divided geographically into several shards, and a committee nodes mechanism is proposed to further reduce energy consumption. In [54], the analytical model of the performance of the wireless Internet of Things (IoT) network was conducted, and the blockchain transaction's success rate and its overall throughput were derived. Xu [55] proposed a framework based on the PBFT and Raft to achieve hyper-reliable decision-making in connected autonomous systems, and its performance is evaluated by the consensus throughout and latency, reliability gain, and node scalability. In [56], the authors proposed a three-stage consensus PBFT for autonomous

driving, where the stages of veto collection and gossip improve communication reliability, and the planning tree stage helps the network select the optimal solution from multiple candidates. Authors in [57] proposed an EigenTrust-based PBFT algorithm. Their algorithm replaces the single primary (an entity in PBFT) with a group of primaries, achieving less view change (a mechanism guaranteeing the liveness of PBFT) probability and communication complexity. Recent work in [58] derived the RAFT reliability in the wireless network, and its performance is indicated by reliability gain and tolerance gain.

However, the relative research on blockchain in the wireless network is yet to be fully developed, as they failed to deploy the blockchain in a more practical wireless network and did not incorporate a wireless protocol such as ALOHA or IEEE 802.11 with CSMA. However, the performance of the PBFT network is restrained a lot by the wireless protocol (i.e. the transmission success probability is greatly reduced when the network size scales up), hence resulting in a lower scalable use case. Initially, consensus mechanisms are designed for wired networks, where the link is reliable and stable, but wireless networks can offer greater accessibility and a larger pool of available nodes. The inherent limitations of PBFT in terms of scalability have restricted its feasibility for large-scale deployment in wireless networks. Therefore, this thesis further proposes a novel framework for deploying PBFT in cellular networks to address these challenges, aiming to enhance node involvement and scalability significantly. Moreover, in the wireless network, participants are not only prone to crashes but also to malicious attacks, which further impair the security of the wireless PBFT network. Hence, a hybrid PBFT network is proposed and investigated.

This thesis aims to explore the feasibility of deploying blockchain technology, specifically PBFT, in the wireless network with the essential decentralised consensus, trust and fault tolerance. Some alternatives or derivatives of PBFT, like Tendermint or Hotstuff, are also efficient in terms of low latency and fault tolerance. They achieve similar levels of liveness and resilience with decentralisation and lower communication overhead. However, if this thesis demonstrates the feasibility of PBFT, it would further validate the viability and effectiveness of them.

1.3 Thesis Outline

The rapid growth of real-time, high-frequency data environments, such as autonomous vehicles and industrial IoT systems, presents unique challenges for

blockchain deployment. Traditional solutions often suffer from high latency and computational inefficiencies, limiting their applicability. This research addresses these limitations by adapting PBFT consensus mechanisms to wireless networks, introducing frameworks like base station-enabled PBFT and hybrid cloud-based models. These solutions reduce communication complexity, enhance scalability, and improve throughput, making them feasible for real-time applications. Numerical results presented in subsequent chapters demonstrate the capability of these frameworks to achieve low latency and high consensus success rates, even under dynamic network conditions. The rest of the thesis is structured as follows:

Chapter 2 provides a foundational understanding of blockchain technology. It demonstrates an overview of blockchain, including consensus protocols, the types of blockchain, and its challenges in deploying in the wireless network. It further introduces wireless consensus networks. Key performance indicators such as security bounds, scalability, throughput, latency, and block generation procedures in Wireless Blockchain Networks (WBNs) are discussed.

Chapter 3 investigates the performance of PBFT in wireless networks using the IEEE 802.11 protocol. This chapter analyses key performance indicators, including consensus success probability, transaction confirmation delay, and view change delay. It also explores scenarios with non-PBFT contending nodes, examining how channel contention affects PBFT performance. Moreover, optimal configurations for packet arrival rates and contention window sizes for maximum network performance are discussed.

Chapter 4 introduces a base station-enabled PBFT network framework, where inter-node communications are facilitated through base stations. It discusses the system models for both single and multiple base station scenarios and compares their performance. The chapter evaluates consensus success probability, communication complexity, average transmit power, view change, throughput and delay. It presents numerical results and optimal configurations for both scenarios, highlighting improvements in scalability, efficiency, and performance with the proposed framework.

Chapter 5 explores the security of a hybrid PBFT network, which consists of a private and a public cloud, in the presence of crashes and malicious attacks. It examines security under decentralised and centralised coordination modes. Numerical results are discussed, showing that hybrid networks offer enhanced security compared to traditional PBFT networks, especially when the private cloud is secure.

Chapter 6 concludes the thesis and outlines future research directions for the development of blockchain technology.

List of Pulications

The research carried out during the course of this PhD has resulted in the following publications:

Journal Paper

- **Z. Zhou**, O. Onireti, H. Xu, L. Zhang, and M. Imran, "AI and Blockchain Enabled Future Wireless Networks: A Survey And Outlook." Distributed Ledger Technologies: Research and Practice (2024).
- **Z. Zhou**, O. Onireti, X. Lin, L. Zhang, and M. Imran, "On the Performance of Wireless PBFT-based Blockchain Network with IEEE 802.11." IEEE System Journal.
- **Z. Zhou**, O. Onireti, X. Lin, L. Zhang, and M. Imran, "Implementing Practical Byzantine Fault Tolerance Over The Cellular Network." IEEE Open Journal of the Communications Society (under review: resubmission)
- **Z. Zhou**, O. Onireti, X. Lin, L. Zhang, and M. Imran, "Security Analysis of the Hybrid PBFT Consensus Network in the Presence of Crashes and Malicious Attacks." (manuscript in preparation).

Conference Paper

- **Z. Zhou**, O. Onireti, L. Zhang, and M. Imran, "Performance analysis of wireless practical Byzantine fault tolerance networks using IEEE 802.11." In 2021 IEEE Globecom Workshops (GC Wkshps), pp. 1-6. IEEE, 2021.
- **Z. Zhou**, Y. Fan, X. Lin, L. Zhang, M. Imran and O. Onireti, "Base Station-enabled PBFT Consensus Network: An Outlook and Performance Analysis." 2024 IEEE 35th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2024.
- X. Lin, **Z. Zhou**, L. Zhang, A. Tukmanov, Q. Abbasi and M. A. Imran, "RIS-Assisted Resource Allocation under Base Stations' Non-Cooperation Scheme." GLOBECOM 2023 - 2023 IEEE Global Communications Conference, Kuala Lumpur, Malaysia, 2023, pp. 7237-7242, doi: 10.1109/GLOBECOM54140.2023.10437328.
- X. Lin, **Z. Zhou**, L. Zhang, A. Tukmanov, Q. Abbasi and M. A. Imran, "Joint Wide Illumination and Null Insertion Design in RIS-

Assisted System." 2024 18th European Conference on Antennas and Propagation (EuCAP), Glasgow, United Kingdom, 2024, pp. 01-04, doi: 10.23919/EuCAP60739.2024.10501227.

- Y. Fan, **Z. Zhou**, Z. Qiao, and L. Zhang, "Decentralized Governance and Technology Integration in DAOs within the Web3 Ecosystem." IEEE Global Blockchain Conference (GBC), 2024.

- Y. Fan, **Z. Zhou**, Z. Qiao, and L. Zhang, "Efficiency Analysis of Decentralized Autonomous Organization (DAO) Voting Mechanisms." (submitted to 2024 IEEE Global Communications Conference).

Chapter 2

Overview of Wireless Blockchain Networks

2.1 Overview of Blockchain

Blockchain technology plays a crucial role in ledger keeping as well as in the cryptocurrency industry. Recently, blockchain technology gained traction from mobile operators, policymakers, and infrastructure commissioners [59]. It is based on a distributed ledger structure, a consensus process. The distributed databases in blockchains are organized by using a hash tree, which is irreversible and also tamper-proof [39, 60]. The structure of blockchain enables the creation of a digital ledger of transactions that can be shared between computers and distributed within the network. Thus, it enables consistency of transactions in the databases while also adding distributed trust. Other attributes of blockchain are that it allows for data integrity, auditability and durability [61]. The consensus mechanism plays an important role in blockchain as it ensures that transactions are ordered unambiguously while maintaining the consistency and integrity of the blockchain across nodes that are geographically distributed. The consensus mechanism, to a great extent, dictates the performance of the blockchain system in terms of the security bound, transaction confirmation delay and throughput, node scalability and energy efficiency performance. In this section, the types of blockchains will be discussed. Furthermore, several main types of consensus algorithms will be introduced: proof of work (PoW), proof of stake (PoS), PBFT, Raft and tangle. Note that other consensus algorithms are either similar to or the derivative of these algorithms, so they will not be included.

2.1.1 Types of Blockchain

In general, blockchain can be divided into three types: public, private, and consortium blockchain.

- *Public Blockchain*: A public blockchain is the most common one, which is open-sourced, and every user can freely participate. Every participant has the right to access the record and add new blocks according to the related consensus algorithm. This type is the most decentralised one with no third party that can supervise or rig it. Every user involved will be automated to maintain this blockchain to gain incentives and avoid the devaluation of its assets. The most well-known examples of public blockchains are Bitcoin [18] and Ethereum [62].

- *Private Blockchain*: Compared with a public blockchain, a private blockchain is more centralised, and participants need permission to join the blockchain and access the data in the blockchain. A private blockchain is usually operated by a single entity. The typical consensus algorithm used in the private blockchain is PBFT, which increases the transaction rates and eliminates the need for incentives. Other consensus mechanisms like Raft have also been implemented recently. For example, some projects within Hyperledger Fabric adopted Raft.

- *Consortium Blockchain*: Consortium blockchains have many similarities with private ones. The biggest difference is that consortium blockchain is run by a group or several entities. For example, the famous project Hyperledger both adopted private and consortium blockchain technology; the most common private blockchain is Ripple (XRP) [63]; while the examples for consortium blockchain usually include Quorum [64] and Corda [65].

2.1.2 Consensus Protocol

Consensus protocols [66, 67] are fundamental to blockchain and are responsible for the generation of a new transaction. Thus, consensus protocols play the most decisive role in the blockchain. There are several options on the consensus mechanism for blockchain, and selecting the right one for a particular application is an important step toward making an efficient and secure blockchain system [39]. In general, consensus protocols can be divided into two categories, proof-based and voting-based.

A proof-based consensus blockchain requires participants to perform sufficient proof tasks before appending a new transaction to the block. The most representative proof-based cases are PoW and PoS. PoW is the enabling technology of the well-known cryptocurrency Bitcoin, whose success over ten years running has proved its robustness. However, its core mechanism requires every participant to solve the hash function, and whichever first gets the solution can write their data into the ledger, generating a new block in the chain and getting the incentive [68]. In other words, the node with the highest computation capability has the greatest chance to generate a new block, which results in a computing power competition.

Many proof-based protocols are proposed as improvements or derivatives of the PoW and PoS or a hybrid form of them, such as delegated proof of stake (DPoS), leasing proof of stake (LPoS), proof of burn (PoB), proof of importance (PoI), proof of capacity (PoC), etc.

In contrast to proof-based consensus, voting-based consensus relies on a democratic process. A new consensus is reached when a certain threshold is achieved. The typical voting-based consensus protocols are PBFT and Raft.

Introduction of the Common Consensus Protocols

Some common consensus protocols used in blockchain are described in the following, including an overview of their suitability for wireless networks.

Proof of Work

Under the protocol of PoW, every node in the network will compete to solve a hash function, such as SHA-256 [18], which requires each node to operate exhaustive computation. The node which gets the value first can write its data into the ledger, generating a new block in the chain and getting the incentive [68]. In other words, the node with the highest computation capability has the greatest chance to generate a new block. The difficulty of the hash function is regulated to maintain the generation of a new block at a constant rate (one block per 10 minutes). If the block is generated faster than the expected rate, the difficulty will increase and vice versa. Besides, the added block in the chain cannot be changed or modified unless the attacker has greater than fifty-one percent computational capacity (51% attack) of the whole network [69]. The most typical application of PoW is Bitcoin, which has been successfully run for over 10 years, showing the robustness of PoW [70].

However, the PoW is a computationally intensive method that consumes a massive amount of power and computing resources. In the wireless network, most devices and users are constrained in terms of computing resources. Moreover, the transaction rate is relatively low, so it is not feasible for wireless networks, which require rapid information exchange and transmission.

Proof of Stake

PoS [71] is another consensus mechanism widely used in Blockchain. Unlike PoW, which is computationally intensive, PoS does not require nodes to compete to solve the hash function. Instead, PoS will randomly select the node to add a new block into the chain, according to the number of coins or assets (this is what stake means). To put it another way, the more coins a node has, the higher the probability it has to generate a new block. This mechanism efficiently reduces the power consumption induced by PoW and saves computing resources.

However, the initial stake accumulation of a node will give it more chances to get coins, resulting in a centralised entity, which is contradictory to the concept of blockchain. What's more, although 51% attack does not exist in PoS, another problem named nothing-at-the-stake attack arises [72]. Those 'wealthy' nodes will put much effort into maintaining the PoS system and stick to the longest chain rule since any attacks and malfunctions will result in the loss of their assets. In comparison, those nodes with few coins will try to cause a fork to get more bonus. Despite the failure, they do not lose much, for they do not have much to lose. Finally, there is no monetary concept in the wireless networks, which rules out the deployment of PoS in wireless networks [72].

Practical Byzantine Fault Tolerance

PBFT [73, 74] is derived from the byzantine fault tolerance algorithm, and as the name suggests, the improvement makes it more practical: PBFT can be tolerant to f number of faulty nodes. In PBFT, every node or replica is involved in the validation execution. A node will be selected as a primary node according to the view-change rule, the node sending the request the is client and the rest nodes are backups. The process involved in PBFT can be divided into several phases in the normal operation case, which consists of pre-prepare, prepare, commit and reply phases, as shown in Fig. 2.1.

After the primary node has received the request from the client by using a point-to-point or broadcast message transfer protocol, the normal case operation starts:

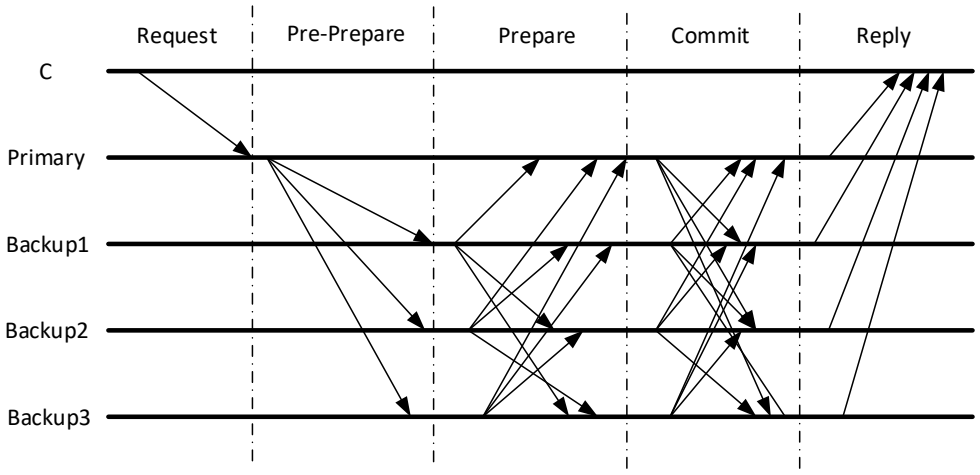

Figure 2.1: The normal case operation of PBFT [73]

- *Pre-prepare:* The primary will forward the pre-prepare message to the backups and the request message is not included to keep the message small.
- *Prepare:* The replica that receives the pre-prepare message will forward the prepare message, the digest of the message $D(m)$, to other replicas. If a replica has received $2f$ prepare that matches the pre-prepare message, the pre-prepare message can be regarded as valid.
- *Commit:* If the prepare message is true, a replica will broadcast the commit message to the rest replicas.
- *Reply:* The reply message received by the client shows the result of the request.

Assume that PBFT is tolerant to f faulty nodes out of n nodes, and faulty nodes can neither non-respond nor give fault messages. A node needs to communicate with at least $n - f$ nodes to ensure the correctness of a message, but f non-responding nodes can also be non-faulty nodes. Thus, $n - f - f > f$, i.e., $n > 3f$ is needed to guarantee the message is correct. Therefore, PBFT can be resilient to up to 1/3 faulty nodes in the network [73].

The fault tolerance and the fact that no computation is needed makes PBFT more competitive. PBFT is incorporated with a view change mechanism, which selects a new primary when the old one fails. This mechanism provides resilience to the PBFT network and prevents a single-point failure. Hence, PBFT has been widely applied in the private and consortium blockchain, such as Hyperledger Fabric [75]. However, as the number of nodes increase, the complexity of the normal case operation of PBFT goes up dramatically, hence making its massive

deployment into the wireless network implausible. The scalability of the PBFT consensus mechanism is limited, and it can only be adopted in small networks.

Raft:

Raft is a consensus algorithm for managing a replicated log [76]. It makes consensus available for more audiences and distributes state machines among the cluster of nodes in the computer system. Every node in the cluster stays in one of the three states: leader, candidate, and follower. The leader can interact with the client, and it receives the requests redirected from the followers; a candidate with the most votes becomes the leader; followers can only talk with candidates or the leader. The Raft will divide the time into arbitrary lengths called terms starting with a leader selection. Raft uses remote procedure calls (RPCs) to carry out the algorithm. "AppendEntries" and "RequestVotes" are two key features of the algorithm.

- *AppendEntries:* The leader initiates these RPCs for state replications.
- *RequestVotes:* A candidate initiates it to ask for votes from the followers at the beginning of each term.

Leader Election Raft introduces a heartbeat mechanism for the leader election. During a term, the leader will periodically send heartbeats to its followers. Suppose a follower does not receive a heartbeat over a specific period called election timeout. In that case, it will consider that the leader is not accessible anymore, and a leader election is needed. After the leader election begins, some followers become candidates and send RPCs RequestVotes to other servers. The election ends if one of the following conditions is satisfied: a leader is elected, or no one wins the election until the election time expires. The candidate who receives the majority of the cluster's vote will be chosen to be the leader. An illustration of the server states for Raft protocol is illustrated in Fig. 2.2.

Log Replication After the leader is determined, the server begins servicing the request from the client. The client's request is composed of several commands that need to be executed by the replicated state machine. The leader will add the request to its log as a new entry and initiate the AppendEntires RPCs to all followers in order to replicate the entry. The leader will continuously send the AppendEntries RPCs to all followers to ensure every node has replicated the entry. The log replication process for the Raft consensus protocol is shown in Fig. 2.3.

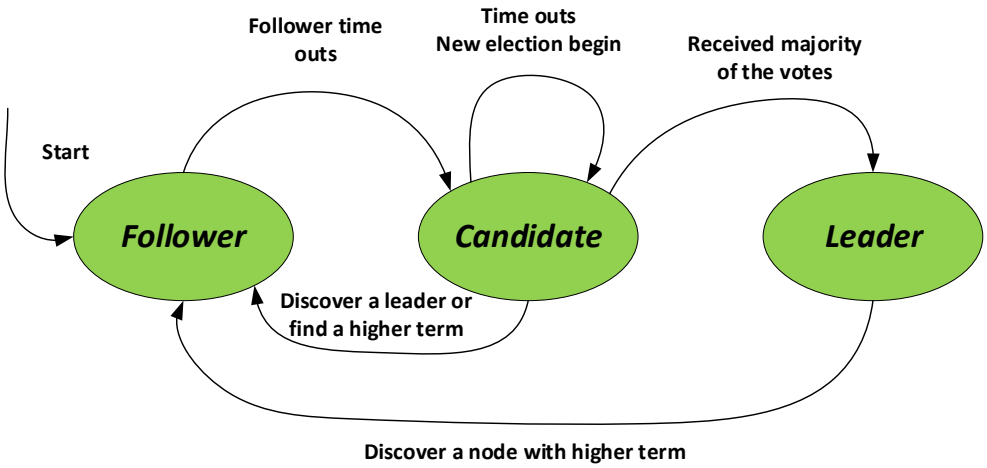

Figure 2.2: Server states in Raft

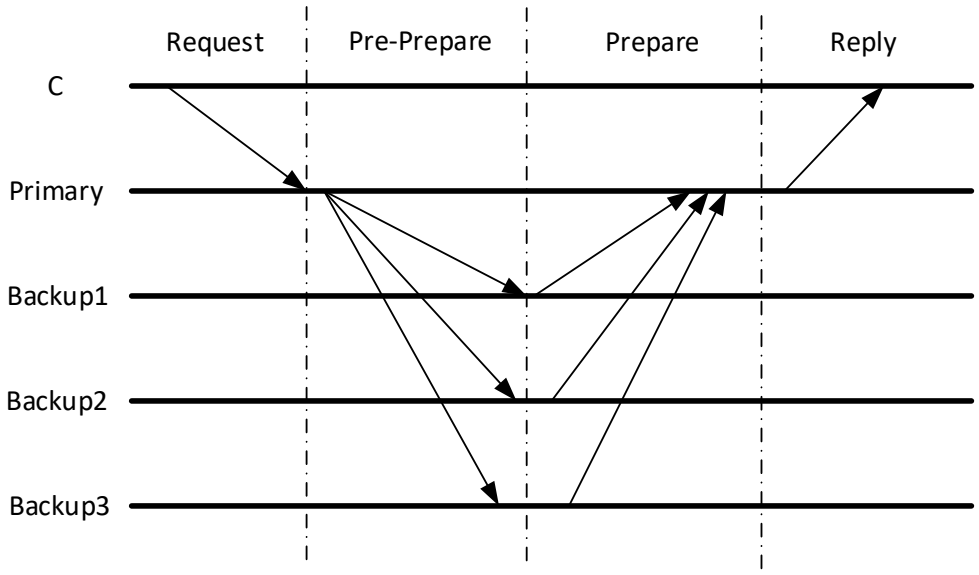

Figure 2.3: The process of log replication in Raft

Cluster Reconfiguration In practice, the system may need to change the cluster's size; for example, exclude some failed nodes or incorporate new nodes. The common method is to shut down the whole system and manually change the configuration, which results in a period of inactivity. Raft introduces an automated configuration method named joint consensus. When the configuration needs to be changed, nodes in the cluster will send the new configuration to each other, and the cluster goes into the joint consensus state when the server can still service the clients. Once all nodes have received the information, the cluster will start using the new configuration.

Log Compaction As the server is servicing the clients in the practical system, the log continues growing taking up a great amount of storage. Hence, this

undermines the efficiency of the entire system. Therefore, Raft incorporates the snapshotting approach to discard obsolete logs, thus achieving log compaction.

According to the above discussion, Raft has many aspects in common with PBFT. Both Raft and PBFT have a particular node referred to as the leader and primary node, respectively. The particular node is responsible for broadcasting the request to other nodes and receiving feedback. However, Raft is not as tolerant to malicious attacks as PBFT, even though it allows node failure. A successful consensus process requires at least 50% of nodes responding [77]. Thus, a malicious attack on the leader node may lead to an entire system shutdown. Besides, Raft's consensus process is much more straightforward than that of PBFT since followers do not need to broadcast the feedback to other followers as PBFT does. This saves the spectrum resources and reduces the complexity, hence making Raft more scalable [78].

Direct Acyclic Graph (DAG) Tangle

Tangle [79] is proposed by Iota for the Internet of Things, using direct acyclic graph technology. Namely, the ledger will increase in a specific direction while the ends will never meet. Moreover, a new ledger is connected to two previous ones. So, it is more like a graph instead of a chain. Compared with other algorithms, tangle breaks the transaction rate barrier, since it does not require computing capability or a validation process. A new block is added to the graph by validating two previous blocks, and it allows parallel validation at the same time. The elimination of waiting time for the previous block and computation requirement make it plausible to validate multiple transactions within a short time. Moreover, tangle does not require transaction fees, which makes it more advantageous. The framework of Tangle is shown in Fig. 2.4.

Tangle uses a tips selection algorithm to determine which transactions are chosen to be validated and add new transactions after the chosen block. This algorithm introduces two types of walks: unweighted and weighted random walks. The unweighted random walk enables the transaction to be selected with equal chance. The weighted random walk embraces cumulative weights, leading to a specific node being selected with a higher probability. This algorithm prevents tangle from the 'lazy' nodes that do not validate the older transaction. Because 'lazy' nodes rarely approve new transactions, it impedes the expansion of the whole tangle.

Although the tangle breaks the low transaction rate's bottleneck and eliminates

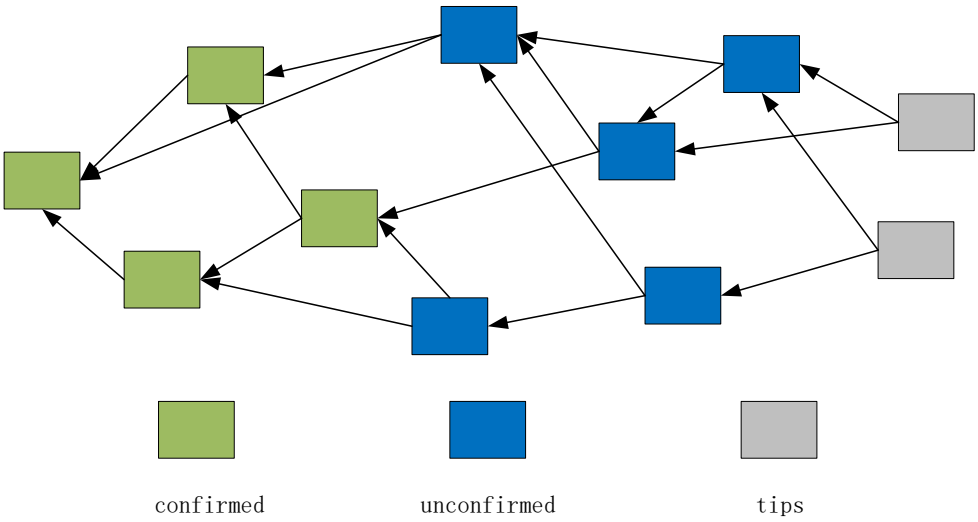

Figure 2.4: Tangle framework [73]

the transaction fees, it still has some problems. In particular, if a node has massive computation capability to create more transactions than the rest of the nodes, it can rig the tangle. Moreover, tangle's security may be compromised in the presence of malicious actors (Sybil nodes) creating fake identities, which can also lead to tangle being manipulated. In order to implement the tips selections algorithm and avoid the aforementioned malicious nodes, Iota employs a coordinator into the tangle. This coordinator introduces a third party, which violates the decentralised scheme of blockchain [82].

Table 2.1 demonstrates the characteristics of the mainstream consensus protocols and also presents their plausibility in wireless networks. Throughput and latency are the most important performance metrics for blockchain deployment in wireless networks. Besides, most mobile devices are computing and storage-constrained; hence, blockchains' computing and storage requirements also have a significant impact. The plausibility of deploying different blockchains in wireless networks can be categorised into three levels. The most appropriate types, like PBFT, which has high throughput, low latency, and low computing requirement, are remarked as 'favoured'. Partially suitable ones are remarked as 'likely'. In contrast, the implausible ones are remarked as 'not likely'.

2.2 Wireless Blockchain Network

The wireless network faces challenges from the openness of the communication channel. In terms of wireless blockchain, take IoT networks as an example, which face both challenges from channel openness, and consensus [55, 83]. Turning

Table 2.1: A Comparison of Commonly Used Blockchain Consensus Mechanisms [66] [80] [81]

Consensus protocol	Accessibility	Scalability	Transaction throughput	Latency	Fault tolerance	Computing needs	Networks needs	Memory needs	Plausibility in WN
PoW	Public	High	Low	High	50% computing power	High	Low	High	Not likely
PoC	Public	High	Low	High	50% storage capacity	Low	Low	Very high	Not likely
PoET	Private	High	High	Low	N/A	Low	Low	High	likely
PoS	Public	High	Low	Medium	50% of stake	Medium	Low	High	Not likely
DPoS	Public	High	High	Low	50% validators	medium	N/A	High	Likely
LPoS	Public	High	Low	High	50% stakes	medium	Low	High	Not likely
PoI	Public	High	High	High	50% importance	Low	Low	High	Likely
PoA	Public	High	Low	High	50% computing power and stake	High	Low	High	Not likely
PoAuthority	Private	medium	High	Low	50% validators	Low	Low	High	Favored
PoB	Public	High	Low	High	50% coins burnt	Low	Low	High	Not likely
PBFT	Private or Consortium	Low	High	Low	33% replicas	Low	High	High	Favored
dPBFT	Private or Consortium	Medium	High	High	33% replicas	Low	High	High	Favored
Raft	Private	Medium	High	low	50% nodes	low	High	High	Favored
DAG	Public	High	High	low	33% computing power	Low	Low	low	Favored

classical consensus, e.g., Raft and PBFT, into wireless consensus [58] can be a feasible solution under the circumstance of a blockchain-enabled wireless IoT ecosystem. The wireless connections among the leader/header and the followers of consensus are vulnerable due to wireless channel fading and unpermitted malicious jammers/noises. Either uplink (UL) or downlink (DL) failure will result in voting failures, thus lowering the transaction/commit success rate. Malicious users can exist in the network to prevent the consensus from being achieved among the nodes through spectrum jamming and flooding the network. Thus, the success rate of blockchain transactions in the presence of radio jamming is a critically important topic to be explored for practical network deployment.

Unlike the traditional communication problems that typically focus on the success of individual communication links, the problem in this study is shifted to multiple communication links network, and the aim is to make sure that the number of successful communication links (for both UL and DL) exceeds the security bound [56], with or without the presence of malicious jamming. To solve this problem, the model of blockchain transaction processing is mapped with the wireless DL and UL transmission. Then, the transaction success probability of wireless consensus is obtained in the study of Raft [84]. Note that the jamming

attacks are from both physical or MAC layers, in the form of pure noise or malicious frames. The study employs the metric of SINR (signal-to-noise-plus-interference ratio) as the chosen threshold, and the SINR threshold can be adapted to any other metrics such as Mean Square Error (MSE) or Bit Error Rate (BER), etc.

In addition to classical consensus, emerging consensus protocols, for instance, multi-layer PBFT [30] provide robust tolerance to nodes and links failures, which makes the communication failure less hazardous compared to the original PBFT consensus. Furthermore, the wireless consensus is also the key to enabling less reliable communication and nodes to achieve ultra-reliable communication and decision [85], as the consensus itself provides the network with fault tolerance in design. By applying the wireless consensus to industrial IoT and critical mission decision-making, reliability can be significantly improved. The most important key performance indicators in the wireless blockchain network are security bound, scalability, throughput and latency.

2.2.1 Security Bound

The security level of the consensus mechanism increases with the number of nodes. Blockchain is run by consensus protocols, and any consensus protocols require validation by every node. For example, PBFT needs at least two-thirds of the nodes' commitment, and Raft needs 50% of nodes' confirmation. Thus, the more nodes a blockchain network has, the safer the blockchain will be. The network coverage determines the number of involved nodes, and usually, the coverage is determined by the base station (BS) deployment and transmitting power. Appropriate node density and power allocation schemes play a significant role in network security.

Moreover, note that many consensus protocols require frequent multicasting, such as PBFT and Raft. Communication quality is another important factor. The collision happening in the communication channel will result in message transmission with some waiting time. This will deteriorate the consensus efficiency or even lead to failure. For example, in the Raft algorithm, each leader only exists for an arbitrary period called a term. To reach a successful consensus process, a leader will continuously resend the AppendEntries RPCs to others until it receives 50% confirmation. Thus, a longer waiting may make a leader not receive enough nodes' confirmation before the term expires. Generally, the communication quality can be enhanced by the multiaccess protocols. Therefore, the multiaccess protocols will also influence the performance of wireless blockchain

networks (WBNs).

2.2.2 Scalability

The scalability of the consensus mechanism [30] is the measure of its capacity to handle an increasing number of nodes. The scalability is mainly determined by the number of communication resources provided. PoW does not require many communication resources, so the PoW-based network's scalability will be determined by the coverage of the wireless network. Hence, the transmission power will largely affect the scalability. However, PBFT's consensus includes a complex communication process, which will consume a great number of communication resources. Thus, a PBFT-based blockchain network is hardly scalable.

2.2.3 Throughput and Latency

The throughput and latency of WBNs are highly correlated. They are most influenced by the type of blockchain protocols deployed and communication resources. For example, the throughput of a PBFT-based network is much higher than a PoW-based network. The bandwidth and spectrum will also influence the throughput and latency of WBNs, especially for the PBFT or Raft-based network, which requires heavy-loaded inter-node communication. Moreover, transmission power is another factor. A high transmission power means broad coverage, so this reduces the need for relays, thus alleviating the latency problem.

2.2.4 Procedures of Block Generation in Wireless Blockchain Networks

The block generation process in WBNs can be divided into four stages: client request, consensus, state replication, and reply to the client. The following will introduce these procedures:

- *Client Request:* This procedure starts with a client request to add a block to the blockchain. More specifically, in the PoW or PoS-based WBN, the client will send its request to at least one miner in the network. Then, all miners will compete for the generation of a new block. In the Raft or PBFT network, the request will be sent to the leader or primary node.
- *Consensus:* The consensus process varies in different WBNs. For example, in the PoW or PoS-based WBN, after the node has received the request from

the client, which is broadcasted to all miners, all miners start to compete for the new block generation, and the winner has the chance to add the new block into the chain. This does not require many communication resources, but it is computing-intensive. However, in the PBFT and Raft networks, frequent inter-node communication is necessary. The primary node or leader will broadcast this request to nodes and gather feedback from them. Thus, these two protocols require substantial communication resources.

- *State Replication:* Once the consensus process has been passed, the authority of the new transaction is verified. A new block will be added to the chain, and this information needs to be broadcast to all nodes in the network. Even though this process does not require as many communication resources as the consensus process does, it requires low latency. Since the information must be transmitted to all nodes within a short time, it may cause forking problems such as in PoW, and undermine the blockchain's effectiveness.

- *Reply to Client:* In the WBN, every client can freely access the blockchain and check if its transaction has been successfully recorded in the blockchain.

2.2.5 Challenges in Implementing Blockchain in Wireless Networks

- *Wireless Coverage:* Since blockchain eliminates the need for the third party's involvement, the network is maintained by all the participants in the network. Moreover, a new block generation needs to be validated by all other nodes. Thus, the more participants involved, the more secure the network will be. The wireless network coverage determines how many participants can participate, and the incentive mechanism determines how many users are willing to participate. Because the competition and computing process of PoW and PoS require substantial resources, an appropriate incentive mechanism is necessary to boost node involvement, guaranteeing the security and effectiveness of the blockchain network.

- *Scalability:* Voting-based consensus blockchain requires frequent communication among the participants, resulting in massive communication overhead, such as PBFT and Raft. As the scale of the network increases, the communication overhead increases exponentially, which consumes a great amount of communication resources and makes such a network less scalable [86, 87].

- *Supervision:* Blockchain is most famous for its decentralised manner, which eliminates the involvement of a central authority. This reduces the risk of privacy leakage and enhances security. However, the elimination of the third party also eliminates the only way of supervision, which increases the entire system's uncertainty. When any malfunction happens, the network will be out of work, and the loss will be irreversible and uncontrollable. What's more, without the central authority, every operation is determinant and based on smart contracts, so this ignores the protection of human rights [88].

- *Storage Limitation:* With the scale of the blockchain, the overall size of the blockchain will be enormous, up to 120GB [89]. This consumes many storage resources and makes it unsuitable for many memory-limited devices, such as smartphones and portable gadgets. This will exclude some participants from the network, thus reducing the effectiveness and security level of the entire network. Even though increasing the single block size can contain more transactions and reduce the overall weight, this measure will make a new block generation more complex, which increases the computation complexity and reduces transaction rates. This also raises the entry requirements for participants. Therefore, the trade-off between the block size and blockchain should be implemented very carefully. Even better is proposing a new protocol that can abandon the obsolete blocks while the robustness of the blockchain will not be influenced.

- *Power Consumption:* Both PoW and PoS have computationally intensive requirements to guarantee the operation of the consensus mechanism [90]. The trade-off between power consumption and privacy is integral to selecting a consensus mechanism for wireless networks. Further, the power consumption will undoubtedly exert more burden on battery capacity-limited devices like smartphones and IoT devices.

- *Computation Requirement:* PoW and PoS require sufficient computing ability in participating nodes [91]. However, most devices in the wireless network are computationally limited.

- *Throughout Constraints:* Due to the computation requirements or validation process, the time taken to generate a new transaction could be too long for many wireless communication systems, especially when low latency is required in such systems [92].

- *Affordability:* A transaction fee or an incentive [93] is necessary for participants to generate new blocks in the PoW and PoS-based blockchain.

However, this is impractical in a wireless network that aims to provide reliable and instant services to users because mobile users need frequent wireless communications, making the expenditure unaffordable.

- *Vulnerability:* Every blockchain has its weak spots. For example, the malfunction of the leader in Raft can result in the whole system being compromised, and the 51% attack [94] in PoW can easily overtake the system, etc. The loss due to such vulnerability could be disastrous for the blockchain-enabled wireless network.

- *Reliability:* Voting-based blockchain heavily relies on the communication link between the nodes [95]. Poor coverage, poor channel condition, or scarce spectrum resources can significantly influence the consensus, which reduces the reliability of the blockchain.

2.3 Integration of Blockchain and Wireless Networks

The 5G technique has facilitated many applications, including industrial automation [96], education [97], mobile health applications [98] and transport [99]. Integrating 5G with blockchain can unlock new decentralised applications while enhancing the security and resilience of wireless applications [100]. The integration of blockchain and wireless networks is mutually beneficial. However, selecting the appropriate type of blockchain is crucial.

As aforementioned, blockchain can be categorised as proof-based and voting-based. Proof-based blockchains are well-known and wildly applied, and the most famous case is Bitcoin, a PoW consensus blockchain whose over 10-year life span has proved its resilience and robustness. However, the mining-based mechanism is computationally intensive, as it requires every participant to compete for a new transaction. Hence, the more powerful a participant is, the more likely it is to succeed in the competition. According to [101], let alone other mining-based blockchains, Bitcoin's electricity consumption can reach up to 80 TWh annually, which accounts for 0.3% of the global electricity consumption. This characteristic makes mining-based blockchain unsuitable for wireless networks, as most mobile participants are computationally limited, and the energy cost is unaffordable. Apart from that, low transaction rates and throughput are other obstacles to the deployment of mining-based blockchain in wireless networks. For instance, the generation rate of bitcoin is mandatorily fixed to approximately every 10 minutes

per block, and the number of bitcoins minted per block is reduced on a four-year basis.

Voting-based blockchains are particularly suitable for wireless networks due to their inherent traits of high throughput and low latency. Additionally, voting-based blockchains are not computationally intensive, making them more appealing to wireless devices. In this context, PBFT emerges as a promising candidate for integrating blockchain with wireless networks. PBFT provides Byzantine fault tolerance, making it suitable for wireless networks where nodes are prone to crashes, failures and potential malicious attacks, thereby enhancing network reliability. PBFT can tolerate up to $\lfloor \frac{n-1}{3} \rfloor$ faulty or non-responsive nodes of the total n nodes in the network, so the security bound of a wireless PBFT network is 1/3. The throughput and latency of PBFT are restrained in the wireless network using the IEEE 802.11 broadcast scheme because of the intense channel contention, which escalates as the network scales up, as presented in Chapter 3. Due to the heavy communication overhead of the normal case operation to reach a consensus, PBFT is restrained to a small-scale network. Hence, this thesis aims to improve the scalability of the wireless PBFT network by proposing a *'timeout'* mechanism with the cellular network, as discussed in Chapter 4. The *'timeout'* also mitigates throughput and latency problems that appeared in Chapter 3. The wireless network not only experiences crashes but also malicious attacks. In addition, even though the view change mechanism guarantees the network's resilience, it also increases the delay of a consensus when a primary node fails, reducing the system's efficiency. A hybrid network that is composed of a secure private cloud and a public cloud is proposed to address the issue in chapter 5.

Chapter 3

PBFT-based wireless Networks with IEEE 802.11

PBFT is a voting-based blockchain that is plausible to be deployed in the wireless network because of its traits of low computational requirement, high throughput, low latency, and essential fault tolerance ability. IEEE 802.11 is a widely used wireless networking standard that allows devices to communicate with each other. Its ease of installation, low cost, and scalability make it ideal for the small-scale local wireless network. In this chapter, the IEEE 802.11 broadcast scheme is incorporated, and the transmission probability is derived based on the Markov chain. The consensus success probability is further analysed and derived based on the transmission success probability. In a realistic wireless network, the spectrum is usually shared, hence introducing a channel contention. This chapter investigates the impacts of channel contention from the non-PBFT nodes on the performance of the wireless PBFT network. The consensus success probability is determined by the network size, contention windows size and packet arrival rates. Contention window sizes influence the backoff counter in the IEEE 802.11 broadcast scheme. An oversized contention window may decrease channel utilisation, and an undersized window may lead to increased collisions. Packet arrival rates influence the channel's overall throughput. Therefore, the optimal configurations of contention window sizes and packet arrival rates for different network sizes are investigated and analysed.

3.1 Introduction

The performance of wireless PBFT networks with IEEE 802.11 and the impact of channel contention, view change delay, and optimal network parameters are highly related. In the real wireless environment, channel contention (CT) from non-PBFT nodes will significantly affect the performance of the wireless PBFT network. Moreover, even though the wireless PBFT network benefits from the liveness and resilience of the view change mechanism, the negative impacts of the view change in terms of delay remain unexplored. The optimal setting of contention window size and packet arrival rate under different network sizes is also worth researching.

This chapter discusses a framework for implementing the PBFT over a wireless channel using the IEEE 802.11 protocol. In this network, the packet arrival pattern follows the Poisson process. The PBFT has to go through the pre-prepare, prepare and commit phases of normal case operation to finish the consensus process. The nodes contend over the wireless channel, and each phase's success probabilities are derived. Moreover, the end-to-end success probability is derived to evaluate the performance and effectiveness of the wireless PBFT network. Transaction confirmation delay, which is the average time between two consecutive successful consensuses, is another metric for evaluating the network's performance. A metric associated with transaction confirmation delay is the throughput, defined as the number of transactions that succeed over a period or the rate of reaching a new consensus. The transmission success rate is determined by three parameters: network size (i.e., the number of nodes), contention window size, and packet arrival rate. Hence, in this work, we derive the optimal window size and packet arrival rate that maximizes the network's throughput without sacrificing the success probability of the PBFT consensus under different network sizes. In this work, we consider implementing PBFT over IEEE 802.11 protocol. Since the IoT application scenarios are among the local networks, the trait of cost-effective and easy installation and efficient coding technique of IEEE 802.11 makes it appealing to the IoT networks.

The PBFT provides liveness guarantee with the view change process. The view change takes effect when the primary in the CM network either becomes a faulty node or breaks down. By selecting a new primary, the view change prevents the whole system from waiting indefinitely. In this regard, we also derive the view change delay in a wireless PBFT network using IEEE 802.11 protocol. Moreover, spectrum in the wireless environment is usually shared by a variety of users, which

Table 3.1: Frequently Used Network Notations in Chapter 3

Transmission success probability	τ
View change delay	D_{vc}
Transmission success probability	P_s
Success probability of prepare phase	P_p
Success probability of commit phase	P_c
End-to-end success probability	P_e
Packet arrival rate	λ
Backoff contention window size	W
Prepare phase's Average medium access delay	$\overline{D_p}$
Commit phase's Average medium access delay	$\overline{D_c}$
Average transaction confirmation delay	$\overline{D_e}$
Non-PBFT contending nodes	n_{ct}
Transmission probability with non-PBFT contending nodes	$\hat{P}_t$
P_s with non-PBFT contending nodes	$\hat{P}_s$
P_e with non-PBFT contending nodes	$\hat{P}_e$
View change delay with non-PBFT nodes	$\hat{D}_{vc}$
Offered load	G

means there will be other nodes contending with the PBFT nodes in the wireless channel. Hence, we show the impact of non-PBFT contending nodes on the wireless PBFT network. The non-PBFT contending nodes do not belong to the PBFT network but share the same spectrum with PBFT nodes. The non-PBFT contending nodes impact the performance by reducing the transmission success probability in all the phases of the normal case operation of PBFT. For example, transmission from non-PBFT contending nodes can collide with the message from the primary in the pre-prepare stage, thus triggering the view change mechanism, which leads to an increase in the average view change delay. The main parameters determining the performance of the IEEE 802.11 wireless PBFT network are the contention window size, denoted as W, and the packet arrival rate, denoted as λ. However, different combinations of W and λ can affect the performance of the wireless PBFT network to a large degree. Therefore, it is important to find optimal pairs for better performance.

3.2 System Model

This chapter considers a distributed system where nodes within the PBFT consensus network are interconnected through the wireless network, utilizing the unsaturated IEEE 802.11 protocol. This section presents the fundamentals of PBFT and the unsaturated IEEE 802.11 protocol. Table 3.1 presents a

comprehensive summary of the frequently appeared notations in this chapter.

3.2.1 Practical Byzantine Fault Tolerance

In a wireless PBFT network consisting of n nodes, ensuring both safety and liveness requires that the number of faulty nodes f does not exceed $\frac{n-1}{3}$. This requirement, as established by Castro and Liskov [73], guarantees that the system remains resilient and operational even when up to $\frac{n-1}{3}$ nodes are faulty, i.e.,

$$f \leq \left\lfloor \frac{n-1}{3} \right\rfloor. \tag{3.1}$$

Denote the set of the PBFT nodes as R, and each node is identified by an integer in $\{0, \ldots, |R|-1\}$. A node is selected as a primary while the rest of the nodes serve as backups. The primary collects the request from the client and broadcasts it to all backups for execution, as illustrated in Fig 2.1. The primary node is selected in a round-robin manner, and only one primary can exist in one view. Hence, when a primary fails, the view change mechanism is triggered to select a new primary. The primary p for the view v can be obtained as

$$p = v \bmod |R|. \tag{3.2}$$

The consensus process follows the phases of the normal operation of the PBFT network [73] described below.

- *Pre-prepare:* Upon receiving the client's request, the primary node broadcasts the pre-prepare message to all backups. This pre-prepare message includes the sequence number n, view number v, and a digest of the message d. The primary also adds the message to its log.
- *Prepare:* Any backups that receive the pre-prepare message validate it. Once a backup node validates the message, it transitions into the prepare phase by broadcasting the prepare message to the other replicas. They append both pre-prepare and prepare messages to their logs.
- *Commit:* Replicas that receive more than $2f$ valid prepare messages broadcast a commit message to any other replicas, and the commit message is true if and only if more than $2f + 1$ commit messages are successfully transmitted.
- *Reply:* Every replica returns the result to the client.

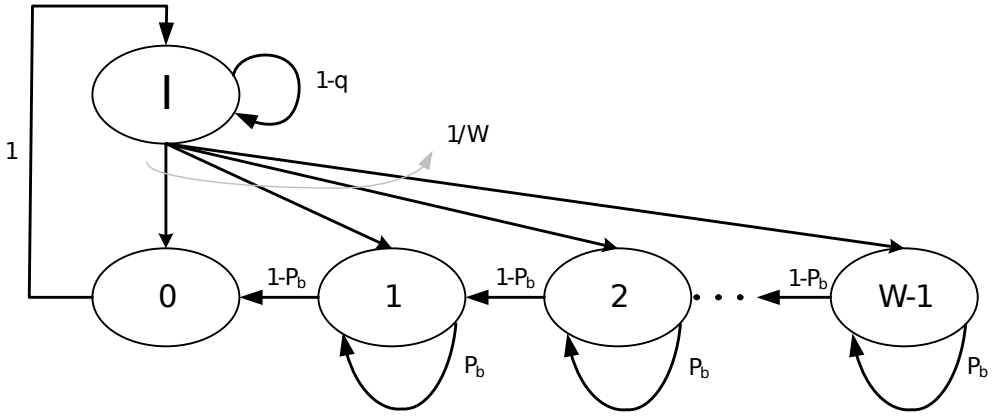

Figure 3.1: Markov chain for unsaturated IEEE 802.11 broadcast [102]

The validity of a request is determined based on receiving a minimum of $f + 1$ identical replies from the network. The client is an IoT device which engages in transactions or information exchange with other IoT devices known as nodes. Once consensus is achieved in the wireless PBFT consensus network, where the nodes are connected using the IEEE 802.11 protocol, the blockchain records the transaction initiated by the client by appending it to a new block.

3.2.2 Unsaturated Broadcast Scheme of IEEE 802.11

It is considered that nodes communicate with other nodes in the wireless PBFT consensus network within a single hop using the IEEE 802.11 broadcast protocol. A realistic PBTF traffic by characterizing the performance of the IEEE 802.11 protocol under unsaturated traffic conditions is further considered. The Markov chain in Fig. 3.1 models the framework's unsaturated IEEE 802.11 broadcast scheme. The wireless PBFT network has n nodes contending for the channel. Since the broadcast scheme of IEEE 802.11 does not include destination information, no RTS/CTS (request to send/clear to send) exchange is incorporated. Thus, without RTS/CTS exchange, the retransmissions will not occur, and the backoff window is always set as the initial minimum backoff size W_{min}. Note that the physical carrier sense still applies even though there is no RTS/CTS exchange. Any node in the wireless PBFT network that receives a packet to transmit initializes a random backoff counter from $\{0, ..., W_{min}\}$. When the medium is sensed idle, the backoff counter is decremented. Otherwise, the node stops decrementing the backoff counter until the medium is free again. A node can only start to transmit when its backoff counter reaches 0. In this model, hidden nodes and capture effects are not considered. Hence, all transmission failures result from collisions.

As aforementioned, a node starts transmission when the counter reaches zero. So the probability τ that a node start transmission in a randomly chosen time slot can be obtained from [102, 103] as

$$\tau = \left(\frac{1}{q} + 1 + \frac{(W-1)}{2(1-P_b)} \right)^{-1}, \tag{3.3}$$

where P_b is the probability that the channel is busy. Given that there are n nodes in the network P_b can be expressed as

$$P_b = 1 - (1-\tau)^{n-1}. \tag{3.4}$$

Further, the parameter q in (3.3) is the probability that there is at least one packet in the buffer waiting for transmission, and it can be expressed as follows:

$$q = 1 - e^{-\lambda E[S_{ts}]}, \tag{3.5}$$

where λ represents the rate at which packets arrive at a node's buffer and $E[S_{ts}]$ is the expected time per slot, which is related to the network parameters.

Let P_t denote the probability that there is at least one node transmitting within the same slot time, where n nodes are contending for the channel. Thus, we can derive the relation between P_t and τ as follow

$$P_t = 1 - (1-\tau)^n. \tag{3.6}$$

Furthermore, a successful transmission occurs only if there is only one node transmitting in a time slot. Thus, the transmission success probability P_s can be expressed as

$$P_s = \frac{n\tau(1-\tau)^{n-1}}{P_t}. \tag{3.7}$$

The expected time per slot $E[S_{ts}]$ in (3.37) can be represented as

$$E[S_{ts}] = (1-P_t)\sigma + P_t(1-Ps)T_c + P_t P_s T_s, \tag{3.8}$$

where σ is the idle slot time, T_s is the average time that the channel is sensed busy because of successful transmission. T_c is the average time that the channel is sensed busy by each node during a collision. Note that we have the same cost for the successful and unsuccessful transmission since the broadcast does not employ

the RTS/CTS mechanism or acknowledgment (ACK) [104]. Hence

$$T = T_s = T_c = \frac{H + E[P]}{R} + DIFS + \delta, \tag{3.9}$$

where δ is the propagation delay, DIFS is the period for a distributed interframe space, and R is the system transmission rate. Note that H is the header length, which is the sum of MAC and PHY headers, and $E[P]$ refers to average packet length. Consequently, by substituting for P_s and P_t from (3.6) and (3.7), respectively, into (3.8), we can express the expected time slot as

$$E[S_{ts}] = (1-\tau)^n \sigma + (1-(1-\tau)^n)T. \tag{3.10}$$

Another important performance metric for IEEE 802.11 protocol is the medium access delay. In this framework, medium access delay refers to the period between when a node starts contending for transmission and when the packet is successfully transmitted [105]. Let D denote the delay, which can be computed as

$$D = T_s + D_s + D_c + T_{slot}, \tag{3.11}$$

where,

- T_s is the time taken for a successful transmission.
- D_s is the average time the channel is in use and thus sensed busy due to the successful transmission of other nodes. Assume there are i successful transmission in a round, then T_s will be

$$D_s = T_s(i-1). \tag{3.12}$$

- D_c refers to the time the channel is sensed busy due to collision, i.e., unsuccessful transmission. Let $P\{N = i\}$ denote the probability that i nodes successfully broadcast their message, for a given number n overall nodes. The delay D_c as a result of collision can thus be expressed from [105] as

$$D_c = \frac{1-(1-\tau)^i - i\tau(1-\tau)^{i-1}}{\tau(1-\tau)^{i-1}} T_c. \tag{3.13}$$

- T_{slot} is the total number of idle time slots and it can be expressed as

$$T_{slot} = \frac{1-\tau}{\tau}\sigma. \tag{3.14}$$

By substituting for D_s, D_c and T_{slot}, from (3.12), (3.13) and (3.14), respectively, into (3.11), we can obtain

$$D = iT_s + \frac{1-(1-\tau)^i - i\tau(1-\tau)^{i-1}}{\tau(1-\tau)^{i-1}}T_c + \frac{1-\tau}{\tau}\sigma. \tag{3.15}$$

3.3 Wireless PBFT with IEEE 802.11

While a PBFT network consisting of n nodes can tolerate up to $\lfloor \frac{n-1}{3} \rfloor$ faulty nodes, it is important to acknowledge that non-faulty nodes may still face challenges in participating in the consensus process due to various wireless network factors, such as poor channel quality, collisions, congestion, etc. Moreover, only transactions agreed upon as valid can be added to the blockchain; hence, the success probability of each transaction in the wireless network determines its overall effectiveness. The analysis considers that the failure is caused by collisions resulting from channel contention when the PBFT consensus network is implemented over the wireless network with IEEE 802.11 protocol. This section focuses on deriving the success probability for each phase of the wireless PBFT network and the overall end-to-end success probability in the normal case operation. Additionally, we calculate the average transaction confirmation delay and throughput for the wireless PBFT network. Next, we show the effect of selecting a faulty primary node by deriving the view change delay.

3.3.1 Wireless PBFT Networks Consensus Success Probability

In the pre-prepare stage, upon receiving the client's request, the primary initializes a new consensus round by broadcasting a pre-prepare message to the other nodes in the network, as illustrated in Fig. 2.1. It is important to note that there is no competition during this phase. Therefore, we assume that only the primary node can access the communication channel, and contention arises after the pre-prepare phase. Denote the number of contending nodes as $\hat{n}$. When the number of contending nodes is one, (3.7) yields a success probability of 100%.

Assumption 1. *Even though there are $\hat{n} = n-1$ contending nodes in the prepare phase, nodes that already received at least $2f$ prepare messages will enter the commit stage and initialize a broadcast of a commit message due to the stochastic nature of the backoff counter. For tractability, we assume that all $\hat{n}$ PBFT nodes*

contend for the channel in the prepare and commit phases. Hence, we employ the same transmission success probability P_s for both phases.

According to the **Assumption 1**, the transmission success probability P_s in the prepare phase can be calculated by (3.7) with $\hat{n} = n$. Let $P\{\hat{n} = i\}$ represent the conditional probability of i nodes successfully receiving the message. This probability is presented as follows:

$$P\{\hat{n} = i\} = \binom{\hat{n}}{i} P_s^i (1 - P_s)^{\hat{n}-i}. \tag{3.16}$$

Theorem 1. *The end-to-end success probability of the wireless PBFT with IEEE 802.11 protocol can be expressed as* (3.17).

$$P_e = \begin{cases} 0 & n < 2f + 1 \\ \sum_{i=2f}^{n-1} \sum_{m=2f+1}^{n} \binom{n-1}{i} \binom{n}{m} P_s^{i+m} (1 - P_s)^{2n-i-m-1} & n \geq 2f + 1 \end{cases} \tag{3.17}$$

Proof. A successful PBFT consensus requires going through all the phases of the normal case operation. Hence, given the fact that there is 100% success probability in the pre-prepare phase, it requires at least $2f$ messages in the prepare phase and $2f + 1$ messages in the commit phase to be broadcasted successfully. Success probability starts to accumulate at prepare phase when more than $2f$ nodes successfully receive the prepare message. Hence, by summing up the conditional probability where the $i \geq 2f$, we can get the success probability of the prepare phase, which can be given by

$$P_p = \begin{cases} 0 & n < 2f \\ \sum_{i=2f}^{n-1} \binom{n-1}{i} P_s^i (1 - P_s)^{n-1-i} & n \geq 2f \end{cases}, \tag{3.18}$$

where P_s is obtained from (3.7) with $\hat{n} = n$ Similarly, the success probability of the commit phase can be drawn by summing up the conditional probability where the $m \geq 2f + 1$, and it can be given by

$$P_c = \begin{cases} 0 & n < 2f + 1 \\ \sum_{m=2f+1}^{n} \binom{n}{m} P_s^m (1 - P_s)^{n-m} & n \geq 2f + 1 \end{cases}. \tag{3.19}$$

Therefore, the end-to-end success probability in (3.17) is obtained by combining P_p and P_c, defined in (3.18) and (3.19). □

3.3.2 Average Transaction Confirmation Delay of Wireless PBFT Network

The transaction confirmation delay is a key performance metric of the wireless PBFT network. It is determined by the underlying consensus mechanism and communication resource provision. In order to obtain its end-to-end evaluation for the wireless PBFT network with IEEE 802.11 protocol, we first introduce the generic medium access delay for the IEEE 802.11 protocol with $\hat{n}$ contending nodes. With i successful transmissions, the expression of the medium access delay can be obtained as [105]

$$D(i) = iT + \frac{1-(1-\tau)^i - i\tau(1-\tau)^{i-1}}{\tau(1-\tau)^{i-1}}T + \frac{1-\tau}{\tau}\sigma, \tag{3.20}$$

where T is the average time the channel is in use due to successful transmissions or collisions [104], and σ is the idle time slot.

Theorem 2. *The average transaction confirmation delay in the wireless PBFT with IEEE 802.11, $\overline{D_e}$, can be expressed as* (3.21).

$$\overline{D_e} = \overline{D_{pp}} + \sum_{i=2f}^{n-1} \binom{n-1}{i} P_s^i (1-P_s)^{n-1-i} D(i) + \sum_{m=2f+1}^{n} \binom{n}{m} P_s^m (1-P_s)^{n-m} D(m) \tag{3.21}$$

Proof. According to the attributes of the PBFT, a transaction is generated when a successful consensus is completed. Hence, the transaction confirmation delay represents the interval in which two contiguous consensus are successfully reached. Considering that the transmission in the pre-prepare phase will always be successful, the delay in pre-prepare phase $\overline{D_{pp}}$ can therefore be obtained by substituting $i = 1$ into (3.20), which further simplifies as

$$\overline{D_{pp}} = T + \frac{1-\tau_0}{\tau_0}\sigma. \tag{3.22}$$

The parameter $\tau_0 = \frac{2q}{2+q(1+W)}$ is the node transmission probability in the pre-prepare phase, which is obtained from (3.3) for the case where $\hat{n} = 1$.

Further, the average medium access delay for prepare phase $\overline{D_p}$ can be given by

$$\overline{D_p} = \sum_{i=2f}^{n-1} \binom{n-1}{i} P_s^i (1-P_s)^{n-1-i} D(i), \tag{3.23}$$

where $D(i)$ is obtained from (3.20).

Likewise, the medium access delay for the commit phase, $\overline{D_c}$, can be expressed as

$$\overline{D_c} = \sum_{m=2f+1}^{n} \binom{n}{m} P_s^m (1 - P_s)^{n-m} D(m). \tag{3.24}$$

Therefore, by combining (3.23) and (3.24), the average transaction delay in (3.21) can be obtained. □

3.3.3 View Change Delay in Wireless PBFT Network

The PBFT protocol employs a series of configurations known as *views*. The view change mechanism is triggered when the primary fails. The view change mechanism ensures the liveness of the PBFT. The selection of a new primary replica follows a round-robin approach, guaranteeing equal opportunities for every node to be the primary. This mechanism prevents backups from indefinitely waiting for request execution.

A backup initiates a timer upon receiving a request, which stops when the request is executed. If a backup does not finish the consensus process before the timer expires, it turns into the view change mode. The view change mode will be initiated when any of the following faulty primary node conditions satisfy [106]:

- nodes receive more than one pre-prepare message containing the same view and sequence number.
- nodes receive a prepare message from the primary despite the primary never sending prepares.

The backups in view change mode broadcast the view change messages to the rest of the PBFT networks. When the new primary in the new view receives more than $2f$ valid view change messages (with the same view, sequence number, and the digest of m) from other nodes, it will send the message to all other nodes. Backups accept it and turn into a new view if the messages from the new primary are properly signed.

Derivation of View Change Delay

As mentioned above, the view change mechanism is incorporated to provide the liveness for the PBFT by allowing the system to progress and preventing the system from waiting indefinitely. When the primary node is out of service, the view change mechanism will be performed in a round-robin manner. However, a

new primary could also be faulty, so it may require up to f consecutive rounds until a non-faulty primary is selected.

Theorem 3. *The view change delay of the wireless PBFT network with IEEE 802.11 protocol is formulated as* (3.25)*, where* $\overline{D_e}$ *is the transaction confirmation delay, which is given in* (3.21)*. The parameter* ζ *is the total timeout for each view, and in this work, it is estimated to be* $2\overline{D_e}$*.*

$$D_{vc} = \begin{cases} \frac{n-1}{n}\overline{D_e} + \frac{1}{n}(\zeta + \overline{D_e}) & f = 1 \\ \frac{n-f}{n}\overline{D_e} + \frac{f}{n}\left((\frac{n-f}{n-1})(\zeta + \overline{D_e}) + \sum_{i=2}^{f}[i \cdot \zeta + \overline{D_e}]\frac{n-f}{n-i}\prod_{v=1}^{i-1}(\frac{f-v}{n-v})\right) & f > 1 \end{cases} \tag{3.25}$$

Proof. Assuming the wireless PBFT network has f faulty nodes, the probability that the selected primary is faulty in a view change is given by $\frac{f}{n}$. When the number of faulty nodes $f = 1$, the average view change delay D_{vc} can be given by

$$D_{vc} = \frac{n-1}{n}\overline{D_e} + \frac{1}{n}(\zeta + \overline{D_e}), \tag{3.26}$$

where $\frac{n-1}{n}$ and $\frac{1}{n}$ are the conditional probability of selecting a non-faulty primary node and a faulty primary node, respectively. For the case where f is greater than 1, when the first selected primary is faulty, the view change process carries on. This leads to a fork whether the next node is faulty and view change continues, or the next node is non-faulty, and the PBFT enters a new view.

In the first case, provided that the probability of selecting a faulty primary at the first round is $\frac{f}{n}$, the probability that the second selected primary is faulty becomes $\frac{f-1}{n-1}$, so the probability that the consecutive two primaries are faulty is given by

$$\frac{f(f-1)}{n(n-1)}. \tag{3.27}$$

In the second case, the probability where a non-faulty node is selected after a faulty primary is $\frac{n-f}{n-1}$. Therefore, the conditional probability of such a case can be expressed as $\frac{f}{n} \cdot \frac{n-f}{n-1}$. By multiplying the delay caused by the one round of view change and transaction confirmation delay, the conditional delay of one round of view change can also be obtained

$$D_{vc}(I = 1) = \frac{f}{n} \cdot \frac{n-f}{n-1} \cdot (\zeta + \overline{D_e}). \tag{3.28}$$

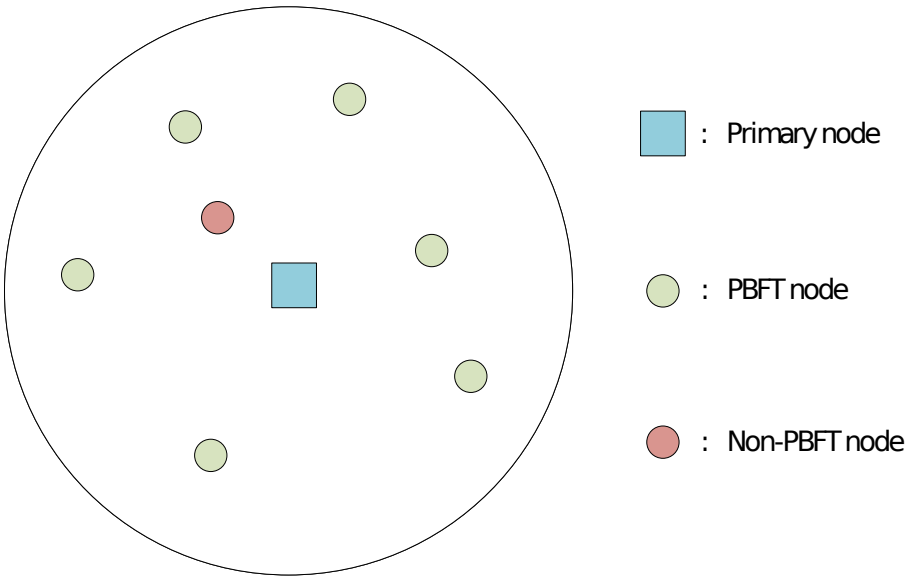

Figure 3.2: Wireless PBFT network with contending nodes

After each former case, a new fork incurs until a non-faulty primary is selected or the maximum number of faulty nodes is reached. Suppose after i consecutive selections of faulty primary, the chance to select a non-faulty one is $\frac{n-f}{n-i}$. Its conditional delay is given by

$$\begin{aligned} D_{vc}(I=i) &= \frac{f}{n}\ldots\frac{f-(i-1)}{n-(i-1)}(i\cdot\zeta+\overline{D_e})\frac{n-f}{n-i} \\ &= \frac{f}{n}\prod_{v=1}^{i-1}\frac{f-v}{n-v}(i\cdot\zeta+\overline{D_e})\frac{n-f}{n-i}. \end{aligned} \tag{3.29}$$

Likewise, by summing up every condition, the lower part of (3.25), shown on the top of this page, is therefore obtained. □

3.4 Case with Non-PBFT Contending Nodes

In this section, we investigate the case where there are other contending nodes in addition to the ones involved in the PBFT consensus network. We refer to these other nodes as non-PBFT contending nodes. Specifically, we will introduce the concept of non-PBFT contending nodes, and how it influences the transmission success probability and view change delay in the wireless PBFT network.

3.4.1 Channel Contention

It has been shown in [107] that, the transmission success probability P_s significantly influences the end-to-end success probability. In this model, the non-PBFT contending nodes share the same attributes as PBFT nodes, apart from not being part of the wireless PBFT network. The schematic network nodes deployment diagram is shown in Fig. 3.2. The PBFT network using IEEE 802.11 comprises the primary and backups, and the non-PBFT nodes introduce additional channel contention. The number of nodes contending for the channel is the most important factor when obtaining the transmission success probability P_s, as the collision is the only factor considered for the packet loss in this work, and more channel contention results in more collisions. Moreover, the wireless spectrum is usually shared in the real wireless network environment, so some other users or nodes contend for the wireless channel with the PBFT nodes. In general, the influence of the non-PBFT contending nodes comes from two aspects:

- The lower transmission success probability: Due to there being more nodes contending the wireless channel, the likelihood of a collision increases, which thus lowers the transmission success probability.
- View change is more likely to happen: The non-PBFT contending nodes constantly contend for the wireless channel, including in the pre-prepare phase. This may result in the primary having a failed broadcast due to collision, which increases the likelihood of the view change.

In this respect, it is worth investigating the impact of channel contention from the non-PBFT nodes on the performance of the wireless PBFT network. For tractability, we assume all non-PBFT contending nodes are also under the IEEE 802.11 broadcast scheme and have the same packet arrival rate as the PBFT nodes.

3.4.2 Wireless PBFT Network with Non-PBFT Contending Nodes

A wireless PBFT network consists of n nodes, and it is assumed that there are $k\%$ additional non-PBFT contending nodes. Let n_{ct} denote the count of non-PBFT contending nodes, calculated as $n_{ct} = \lceil k\% \cdot n \rceil$, hence, the total number of wireless channel users becomes

$$\overline{n} = n + n_{ct}. \tag{3.30}$$

A transmission only succeeds when only one node tries to use the channel. Hence, the transmission success probability $\hat{P}_s$ is given by

$$\hat{P}_s = \frac{\overline{n} \cdot \hat{\tau}(1-\hat{\tau})^{\overline{n}-1}}{1-(1-\hat{\tau})^{\overline{n}}}. \tag{3.31}$$

Note that **Assumption 1** also holds in this case; thus, it is assumed that both the prepare and commit phases share the same success probability denoted as $\hat{P}_s$. The conditional probability $P\{N=i\}$ in such phases, representing the probability of i nodes successfully broadcasting their messages, can be expressed as

$$P\{N=i\} = \binom{n-1}{i} \hat{P}_s{}^{i} (1-\hat{P}_s)^{n-1-i}. \tag{3.32}$$

Theorem 4. *The end-to-end success probability of the wireless PBFT with n_{ct} non-PBFT contending nodes can be expressed as in* (3.33)*. The parameter $\hat{P}_{s_{pp}}$, which is defined later in* (3.35)*, is the success probability in the pre-prepare phase.*

$$\hat{P}_e = \begin{cases} 0 & n < 2f+1 \\ \hat{P}_{s_{pp}} \cdot \sum_{i=2f}^{n-1} \sum_{j=2f+1}^{n} \binom{n}{i}\binom{n}{j} \hat{P}_s{}^{i+j} (1-\hat{P}_s)^{2n-2-i-j} & n \geq 2f+1 \end{cases} \tag{3.33}$$

Proof. In the pre-prepare phase, the pure wireless PBFT network without non-PBFT contending nodes can reach 100% success probability since only the primary in this phase uses the wireless channel and broadcasts the request from the client to the whole network. However, the wireless PBFT network with other non-PBFT contending nodes will not achieve 100% success, as the non-PBFT contending nodes also contend the channel with the primary in this phase. The success probability in the pre-prepare phase for the case with contending node is denoted by $\hat{P}_{s_{pp}}$. Suppose the primary fails to broadcast in this phase after a timeout. In that case, the backups will perceive the primary node as being faulty, thus initiating the view change protocol to select a new primary for the new round of the consensus process. On the other side, if the primary successfully broadcasts the client's request to the entire network, the normal case process of PBFT will be carried out.

Once it goes into the prepare phase, the proof follows the same process in **Theorem 2**. □

3.4.3 View Change Delay in Wireless PBFT with Non-PBFT Contending Nodes

As aforementioned, increased channel contention also increases the probability of view change occurring. In pre-prepare stage, only the primary and the non-PBFT contending nodes are active such that $\hat{n} = 1 + n_{ct}$; the transmission probability of this phase $\hat{P}_{t_{pp}}$ is expressed as follows

$$\hat{P}_{t_{pp}} = 1 - (1 - \hat{\tau})^{1+n_{ct}}, \tag{3.34}$$

where $\hat{\tau}$ is obtained from (3.3) with $\hat{n} = 1 + n_{ct}$. Then, the transmission success probability of the pre-prepare stage $\hat{P}_{s_{pp}}$ for the case with n_{ct} non-PBFT contending nodes can be formulated as

$$\hat{P}_{s_{pp}} = \frac{(1 + n_{ct})\hat{\tau}(1 - \hat{\tau})^{n_{ct}}}{\hat{P}_{t_{pp}}}. \tag{3.35}$$

Therefore, the view change delay in wireless PBFT network with non-PBFT contending nodes, $\hat{D}_{vc}$, can be expressed as

$$\hat{D}_{vc} = \frac{D_{vc}}{\hat{P}_{s_{pp}}}, \tag{3.36}$$

where D_{vc} is given in (3.25).

3.5 Optimal Packet Arrival Rate and Contention Window

The transmission success probability in the IEEE 802.11 wireless PBFT network depends on two key factors: W and λ. The network's performance exhibits significant variation across different combinations of W and λ. Hence, this section presents the problem formulation and algorithmic description of W and λ. Note that though the focus is on the case without non-PBFT contending node, the analysis can be easily generalised.

3.5.1 Problem Formulation

Provided the λ and the expected time per slot $E[S_{ts}]$, the packet arrival probability q in (3.3) can be well approximated as follows in the situation where

each node can only buffer one packet [102]

$$q = 1 - e^{-\lambda E[S_{ts}]}. \tag{3.37}$$

Hence, from equations (3.3), the transmission rate τ can be transformed to

$$\tau = \left(\frac{1}{1 - e^{-\lambda E[S_{ts}]}} + 1 + \frac{(W-1)}{2(1-\tau)^{\hat{n}-1}} \right)^{-1}, \tag{3.38}$$

where $E[S_{ts}]] = (1-\tau)^{\hat{n}}\sigma + (1-(1-\tau)^{\hat{n}})T$ according to [108], which is a function of the transmission rate τ and $\hat{n}$ nodes. Consequently, the parameter τ is determined by three parameters: $\hat{n}$, which are the number of nodes contending for the channel, W, and λ.

In this respect, if the optimal τ is obtained under different network sizes, the pairs of W and λ can be calculated by applying W from the set $\{0, ..., W_{min}\}$, and W can only be selected from the set $\{32, 64, 128, 256\}$. The optimal value is further determined for a better throughput-delay trade-off.

3.5.2 Algorithmic Description

As shown in equations (3.17) - (3.18), the success probability is the sum of a set of binomial distribution $B(n, P_s)$ which can be generalised as

$$B(\hat{n}, P_s) = \binom{\hat{n}}{i} {P_s}^i (1 - P_s)^{\hat{n}-i}. \tag{3.39}$$

Thus, the maximum value of each element in the binomial distributions should be found to maximize the probability of success. The normal distribution can be used as an approximation of binomial distribution, according to a particular case of the central limit theorem, the De Moivre-Laplace theorem [109]. In this case, as the sample size $\hat{n}$ increases, if the probability P_s is between 0 and 1, the binomial distribution approaches normal distribution with a mean of $\mu = \hat{n}P_s$ and standard deviation of $\sigma = \sqrt{\hat{n}P_s(1 - P_s)}$.

By introducing the formula of the normal distribution, i.e.,

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2}, \tag{3.40}$$

Algorithm 1 Procedures for optimal pairs of W and λ

Input: $F(n,\tau), P_b(\tau), P_t(\tau), P_s(\tau), E[s_{ts}]$
Output: $\{W^*, \lambda^*\}$

$\tau^* \leftarrow F(n,\tau)$
$P_b^* \leftarrow P_b(\tau^*)$
$P_t^* \leftarrow P_t(\tau^*)$
$P_s^* \leftarrow P_s(\tau^*)$
$E[s_{ts}]^* \leftarrow E[s_{ts}](\tau^*)$
$\tau(W,\lambda) \leftarrow (2) \leftarrow P_b^*, P_t^*, P_s^*, E[s_{ts}]^*$
for $\lambda = 1$ **to** 117 **do**
    $\{W\} \leftarrow \tau(W,\lambda)$
end for
for $W \in \{W\}$ **do**
    if W is close to elements in $\{32, 64, 128, 256\}$ **then**
        $\{W\}^*$ appends W
    end if
end for
Return $\{W\}^*$
if length of $\{W\}^*$=1 **then**
    $W^* = \{W\}^*$
else
    $W^* = max\{W\}^*$
end if
$\lambda^* \leftarrow \tau(W^*,\lambda)$
Return $\{W^*, \lambda^*\}$

the expression (3.39) can be transformed to

$$B(\hat{n}, P_s) = \frac{1}{\sqrt{2\pi\hat{n}P_s(1-P_s)}} e^{-\frac{(x-\hat{n}P_s)^2}{2\hat{n}P_s(1-P_s)}}. \tag{3.41}$$

Furthermore, the cumulative distribution function (CDF) of the normal distribution is

$$\phi(x) = \frac{1}{2}\left(1 + erf\left(\frac{x-\mu}{\sigma\sqrt{2}}\right)\right). \tag{3.42}$$

By substituting μ and σ, it becomes

$$F(x, P_s) = \frac{1}{2}\left(1 + erf\left(\frac{x-\hat{n}P_s}{\sqrt{2\hat{n}P_s(1-P_s)}}\right)\right). \tag{3.43}$$

It is worth noting that the probability starts to sum up when the number of nodes equals $2f$. Thus, by substituting x with $\hat{n} - 2f$, and P_s with $\frac{\hat{n}\tau(1-\tau)^{\hat{n}-1}}{1-(1-\tau)^{\hat{n}}}$, (3.43)

Table 3.2: Optimal τ for different n

Number of nodes	Optimal τ	Number of nodes	Optimal τ
4	0.0201	20	0.0080
5	0.0262	25	0.0063
6	0.0302	30	0.0070
7	0.0124	35	0.0058
8	0.0162	40	0.0050
10	0.0098	45	0.0054
12	0.0142	50	0.0047
15	0.0117	100	0.0030

can be transformed to

$$F(\hat{n},\tau)=\frac{1}{2}\left(1+ erf\left(\frac{\hat{n}-2f-\frac{\hat{n}^2\tau(1-\tau)^{\hat{n}-1}}{(1-(1-\tau)^{\hat{n}}}}{\sqrt{2\frac{\hat{n}^2\tau(1-\tau)^{\hat{n}-1}}{(1-(1-\tau)^{\hat{n}}}\left(1-\frac{\hat{n}\tau(1-\tau)^{\hat{n}-1}}{(1-(1-\tau)^{\hat{n}}}\right)}}\right)\right). \tag{3.44}$$

The CDF is thus obtained as a function of $\hat{n}$ and τ. In order to acquire the optimal value of τ for a network comprising $\hat{n}$ contending nodes, the value of the parameter $\hat{n}$ can be substituted into (3.44) to obtain the phase (prepare or commit) success probability as a function of τ, i.e., $F(\tau)$. Consequently, the optimization problem can be defined as

$$\begin{aligned} \underset{\tau}{\text{minimize}} \quad & -F(\tau) \\ s.t. \quad & f \leq \lfloor \tfrac{n-1}{3} \rfloor \\ & 0 \leq \tau \leq 1 \\ & 0 \leq F(\tau) \leq 1. \end{aligned} \tag{3.45}$$

The first constraint in (3.45) is a requirement for the PBFT network in terms of the number of faulty nodes allowed in the network. Moreover, the second and third constraints are probability events which are constrained between zero and one. The optimization function with the objective function and constraints defined in (3.45) can be effectively solved by employing the classic interior-point method [110], which is incorporated within the built-in function "fmincon" in Matlab. To maximize the performance of the wireless PBFT network, τ should be as large as possible. TABLE 3.2 shows some examples of the optimal τ under different selected PBFT networks with n nodes. The value of the optimal τ does not go down as smoothly as the n goes up. This phenomenon can be attributed to the constraint mentioned in (5.1), where the number of faulty nodes may not increase proportionally with the network scale, as it has to be an integer ($f = 1$

when $n = 4, 5$ and 6, and it becomes 2 when $n = 7$).

With the optimal τ value obtained for an n-nodes PBFT network, the parameters P_s as defined in (3.7), P_b and $E[S_{ts}]$ become constant values. Consequently, (3.3) turns to a function of the W and λ. The offered load, G, is usually used to measure the traffic of a network. According to [102], the offered load indicates the usage of the wireless channel rate, and it can be calculated by the packet bit rate transmitted divided by the channel bit rate in a unit of time as,

$$G = \frac{\lambda(E[P] + H)}{R}, \tag{3.46}$$

where $E[P]$ is average packet length, H is the header, and R is the channel bit rate. Therefore, by applying the parameters in [107] to (3.46), it can be obtained that $\lambda = 117.59$ when the offered load $G = 1$. Hence, it is assumed that the network reaches the full load when λ equals to 117, as illustrated in Fig. 3.3.

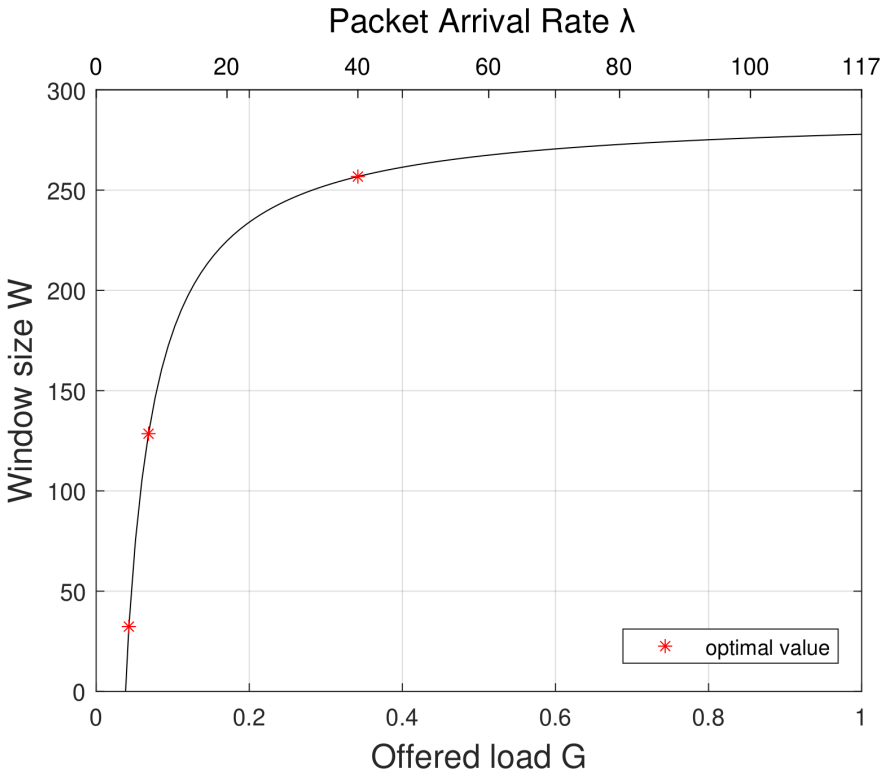

Figure 3.3: Optimal pairs of W versus offered load G with $\tau = 0.0059$ and $n = 28$

Fig. 3.3 provides the correlation between the W and the λ that satisfies the optimal τ. The curve shows that W and λ are positively correlated. However, the W is restricted to the power of 2, normally from $\{32, 64, 128, 256\}$. Therefore, the optimal pairs of W and λ can be calculated through the restriction of W. The largest pair will be the most suitable for a network with multiple pairs of W

Table 3.3: Network Parameters

MAC header	24 bytes
PHY header	16 bytes
Payload size	1023 bytes
Channel Bit Rate	1 Mbits/s
Propagation Delay δ	1 μs
Slot time σ	20 μs
SIFS	10 μs
DIFS	50 μs

and λ. Because under the same success probability, a more considerable packet arrival rate means higher throughput and, hence, better network performance. Algorithm 1 describes the steps for obtaining the optimal pairs of W and λ.

3.6 Numerical Results and Discussion

Section presents the simulation and analytical results. The details of the network parameters are given in Table 3.3.

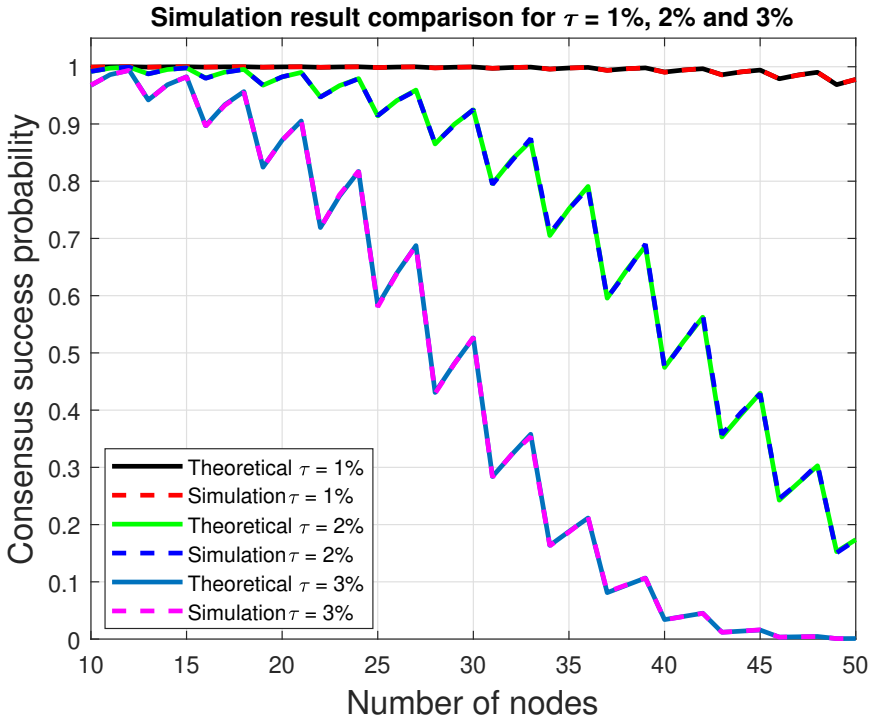

Figure 3.4: Analytical and simulation result comparison when $\tau = 1, 2, 3\%$, respectively

Fig. 3.4 plots the simulation and analytical results of the consensus success probability against the number of nodes n when the transmission probability of

each node is 1%, 2%, and 3%. The simulation result is obtained by averaging 1000000 trials. The model's validity is confirmed through the tight match between the simulation and analytical results.

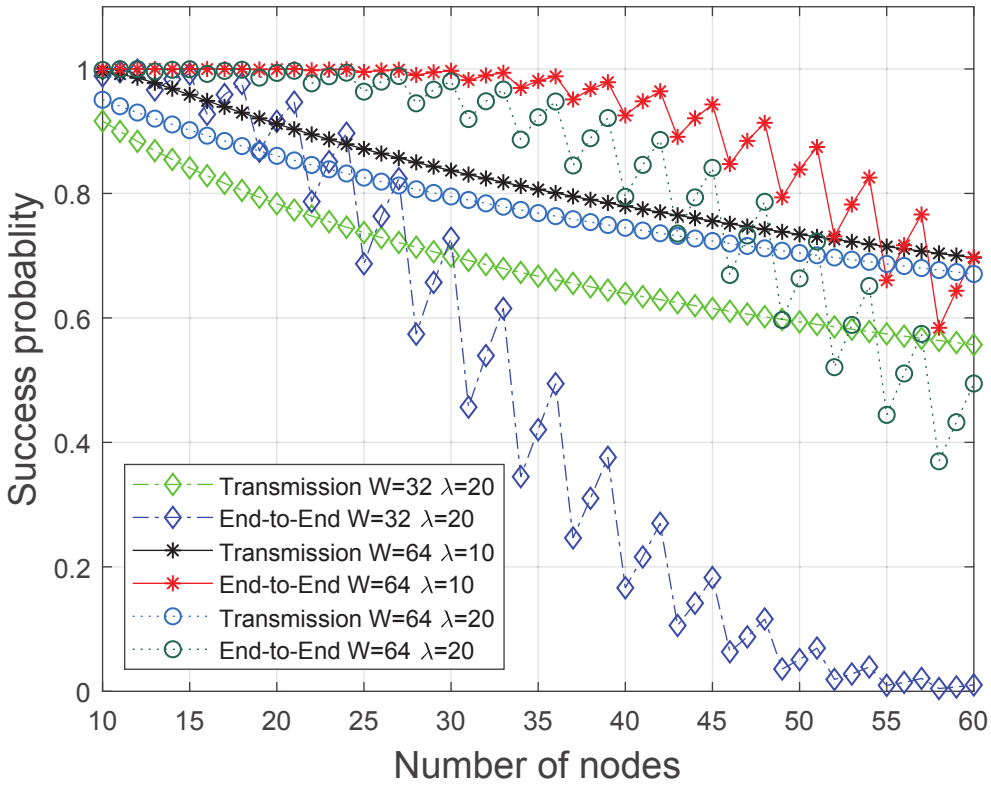

Figure 3.5: Success probability comparison of the wireless PBFT network

To explore the impact of the packet arrival rate λ and the contention window size W on the success probability, λ is reduced to 10, i.e., $[W = 64, \lambda = 10]$, and W to 32, i.e., $[W = 32, \lambda = 20]$ as shown in Fig. 3.5. The plot for the network with $[W = 64, \lambda = 20]$ is also shown as the benchmark. In Fig. 3.5, even though the transmission success probability difference from the benchmark is marginal (less than 0.1), the end-to-end transmission success probability experiences a huge difference. The lowest point on the plot of the end-to-end success probability for the network with $[W = 64, \lambda = 10]$ (red line) is around 0.6, while that of the network with $[W = 32, \lambda = 20]$ (blue line) reaches 0. Furthermore, it can be seen that the end-to-end success probability of the wireless PBFT network is very sensitive to the transmission success probability P_s when $P_s < 0.84$, which is referred to as the critical point. So, we can have a hypothesis that W has a stronger impact on the wireless PBFT networks' performance. The results in Figs. 3.6 and 3.7 have validated this hypothesis. From Fig. 3.6, where $\lambda = 20$, it can be seen that W has a great influence on the success probability, which remains nearly 100% for $W = 128$. It can be seen that reducing W by a factor of half

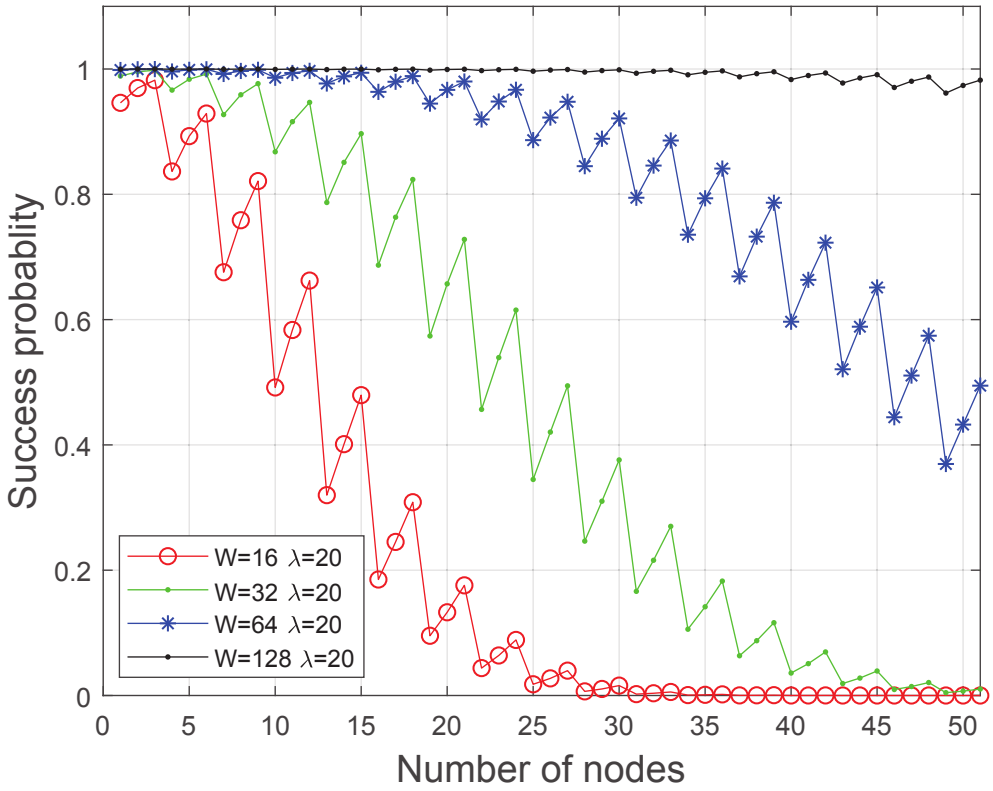

Figure 3.6: End-to-end success probability for different window size W and fixed packet arrival rate $\lambda = 20$

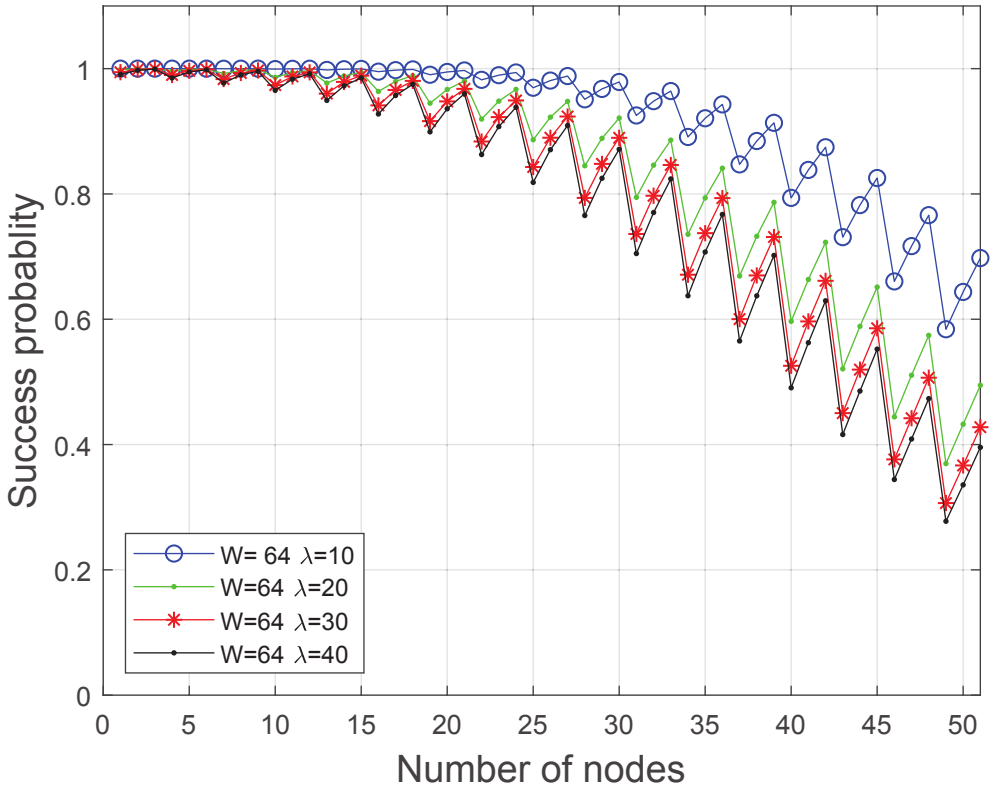

Figure 3.7: End-to-end success probability for different packet arrival rate λ and fixed window size $W = 64$

leads to a significant reduction in the end-to-end success probability. Especially, the case with $W = 16$ hits zero end-to-end success probability when the number of nodes only equals 25. This means the wireless PBFT network under such parameters has poor scalability. However, the difference in Fig. 3.7 where the contention window size is fixed to $W = 64$ can be seen to be marginal.

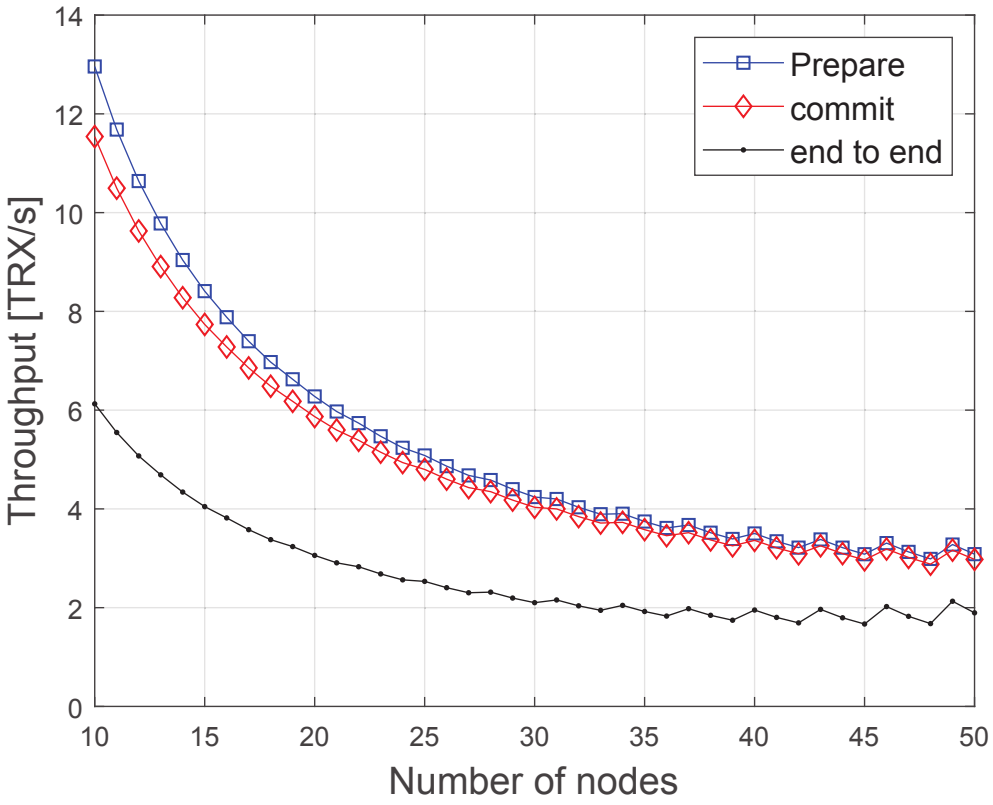

Figure 3.8: Transaction throughput versus number of nodes with $\lambda = 20$ and $W = 64$

Figs. 3.8 and 3.9 show the relationship between the transaction throughput and transaction confirmation delay of wireless PBFT network and the numbers of nodes. Since the throughput and delay are highly related, the discussion focuses on the throughput. In Fig. 3.8, after experiencing a sharp decline, it can be seen that the transaction throughput starts to converge to a fixed value when the number of nodes reaches 30. Thus, combining this with other results presented earlier above, the performance when designing wireless PBFT network using IEEE 802.11 protocol can be maximised.

Fig. 3.10 illustrates the end-to-end success probability of the wireless PBFT network under a different percentage of non-PBFT contending nodes. The zig-zag pattern observed in the plots can be attributed to the nonlinear rise in the number of faulty nodes, resulting in an unsteady progression, and this also applies to Fig. 3.11 and Fig. 3.13. It is worth noting that despite the marginal variation

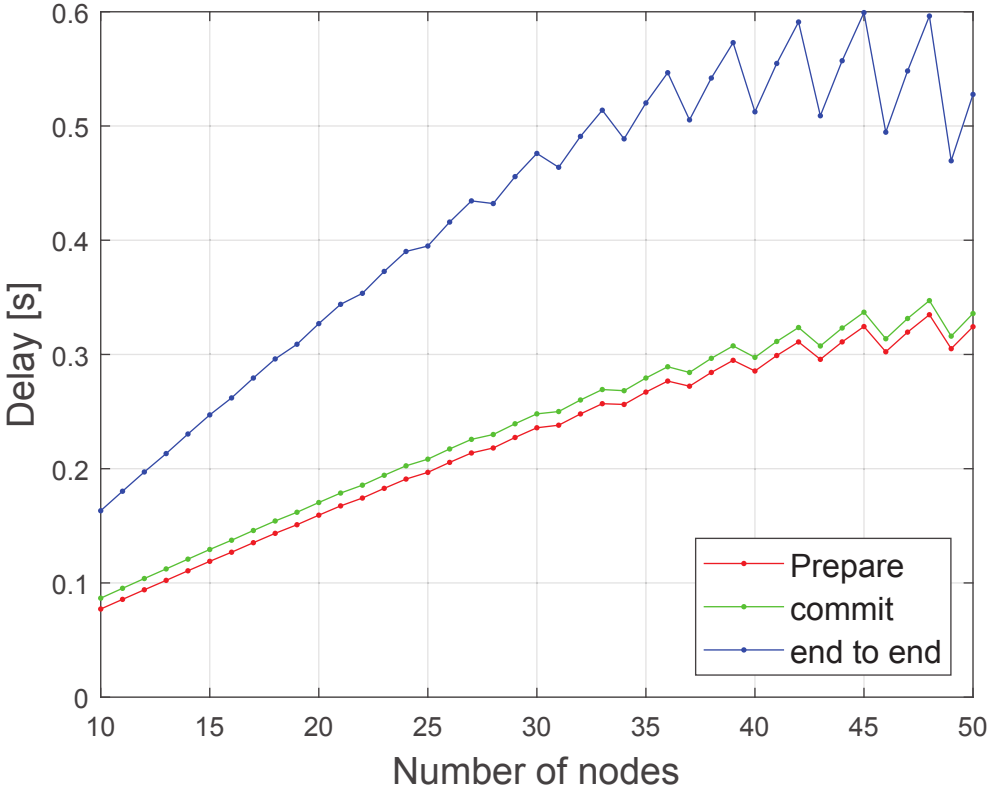

Figure 3.9: Transaction confirmation delay versus number of nodes with $\lambda = 20$ and $W = 64$

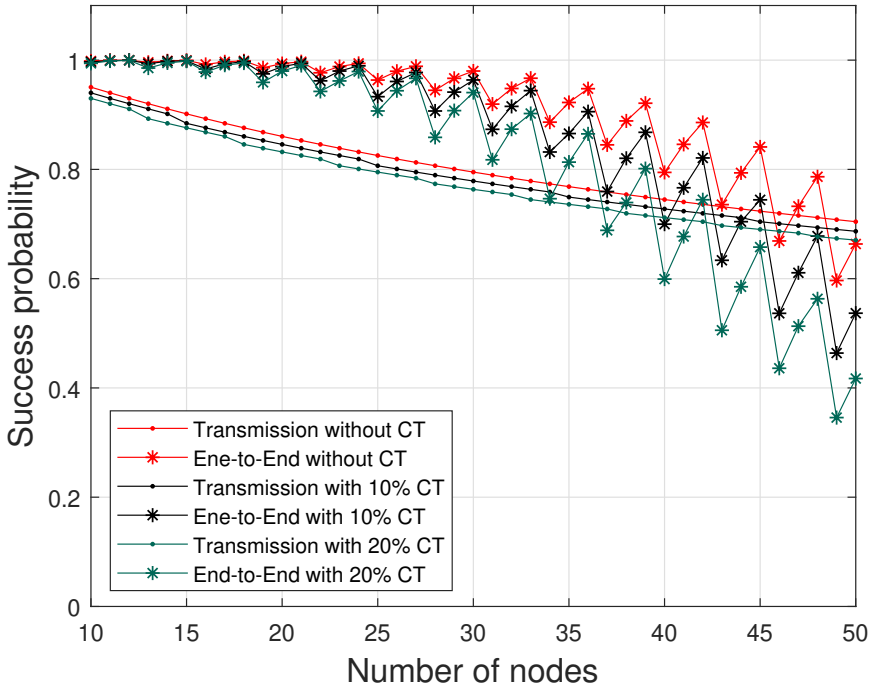

Figure 3.10: Success probability with non-PBFT contending nodes for $\lambda = 20$ and $W = 64$

(around 0.02) in the transmission success probability under each scenario, the difference in the end-to-end success probability is significant, particularly when the network size increases to 50 nodes, where the difference becomes nearly 0.1. This result matches the conclusion from [107] that a slight change in transmission success rate can significantly degrade the wireless PBFT network. Therefore, it is essential to have a dedicated wireless network for PBFT when designing a wireless PBFT network.

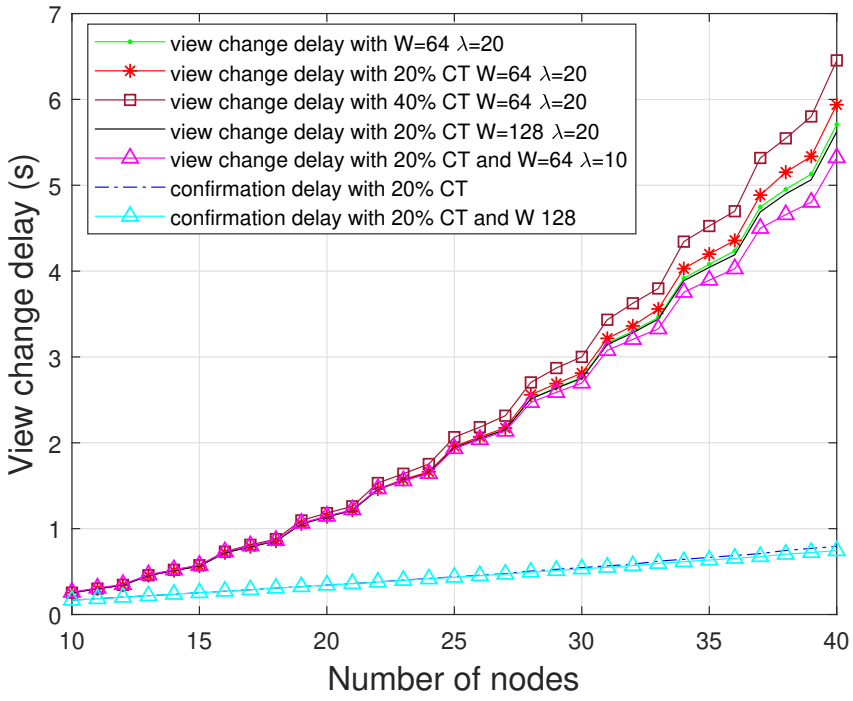

Figure 3.11: View change delay with 0%, 20% and 40% non-PBFT contending nodes versus transaction confirmation delay for different W and λ

Fig. 3.11 presents the view change delay versus the number of nodes. In scenarios where the number of nodes is small, the disparity between the view change delays and the transaction confirmation delay is marginal, where the view change delays are around 0.253, while the confirmation delay is around 0.167. However, with a growing number of nodes, the average view change delay exhibits an exponential increase while the transaction confirmation delay increases linearly. Considering the impacts of non-PBFT contending nodes, the increase in view change delay is subtle. This indicates that channel contention from non-PBFT nodes has limited influence on the view change delay, and the attribute of the PBFT protocol and transaction confirmation delay mainly determines the view change delay. Primary node selection for the view change is done only within the PBFT network. So the probability of selecting a faulty primary stays the same. The impact on the

view change delay is primarily attributed to the additional channel contention from the non-PBFT nodes, which causes the transmission success probability P_s to drop.

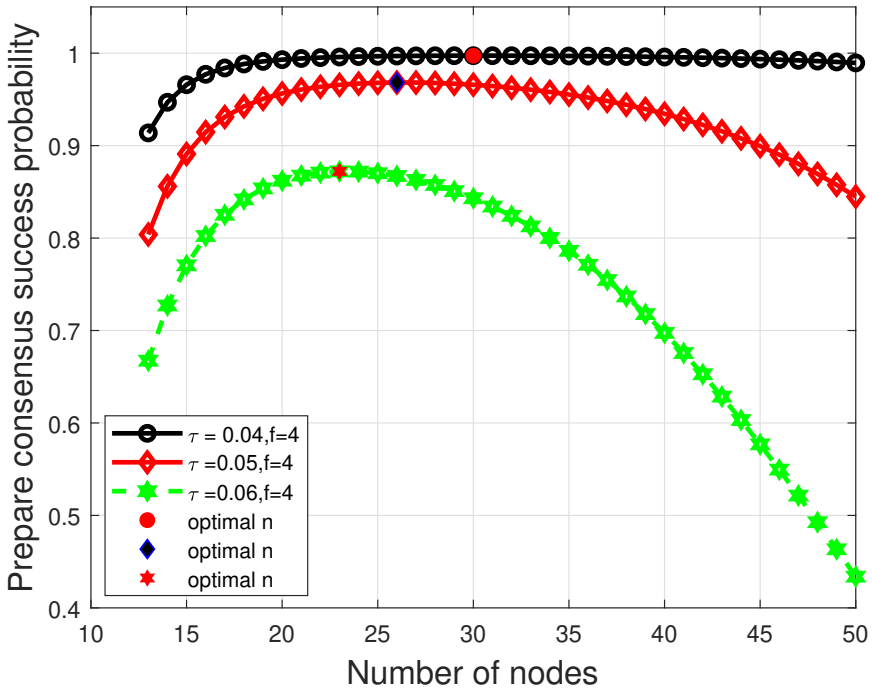

Figure 3.12: Prepare phase consensus success probability against number of nodes for different τ and fixed faulty nodes

Fig. 3.12 presents the effects of different τ on the success probability for the case with $f = 4$. It can be seen that there exists an optimal number of nodes that maximizes the success probability for the case with $\tau = 0.04$, 0.05, and 0.06. This is due to the fact that collisions are more likely to happen as the number of nodes increases. The increase before the optimal point can be attributed to the increase in the number of non-faulty nodes. Note that the impact of the collisions becomes more predominant as the number of nodes further increases.

Fig. 3.13 presents the pairs of λ and $W = 32, 64$ and 128 that satisfy the optimal τ. It is worth noting that the scenario where $W = 256$ is excluded, as most of its results do not fall in the feasible domain, and the results only become valid when the network grows to a relatively large scale. As shown in Fig. 3.13, λ gradually goes down as the network becomes larger. This phenomenon can be attributed to the fact that to maintain τ at a constant level, each node in the network should have fewer packets to transmit (hence, fewer packets arriving in the network). W also holds significance in determining the value of λ. Each time W doubles, the network is capable of receiving more packets. This relationship

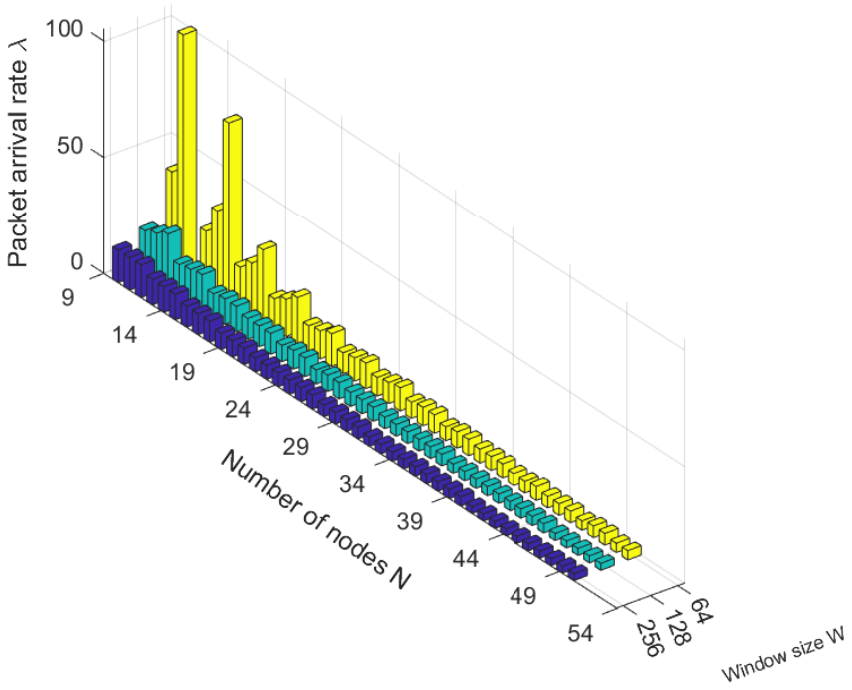

Figure 3.13: 3D plot of pairs for λ and $W = 32, 64$ and 128 under different numbers of nodes

arises because as the value of W increases, the average waiting time for a node to initiate a transmission also experiences a corresponding increase. This indicates the network that has more buffer for the incoming packets, therefore, is able to handle a higher λ.

As aforementioned, λ can benefit from a larger W. Even though the optimal τ can be achieved by multiple pairs of λ and W, the pair with higher λ is more appealing as it contributes to higher throughput for the wireless PBFT network. Hence, Fig. 3.14 presents the optimal pairs of W and λ that maximize the throughput. When the network scale is relatively small (i.e. n from 10 to 25), the optimal W is 128, and when the scale is large (i.e. n from 37 to 50), the optimal W is 256. The optimal W fluctuate between 128 and 256 when n is between 25 and 37. This phenomenon arises from the inconsistent increment of the number of faulty nodes compared to the overall number of PBFT nodes. There are minor exceptions when $n = 29$ and 30, where the optimal W is 32. This is because as the value of the λ increases, the corresponding W for the optimal τ also increases, as shown in Fig. 3.3. At the points of $n = 29$ and 30, the elements of the W are closer to 32. Hence, for a better τ, the optimal pairs with the value of $W = 32$ are obtained. The shape of the optimal τ plot also reflects the impact of the quantity of faulty nodes. The black plots show the optimal W when $\lambda = 30$, and it is

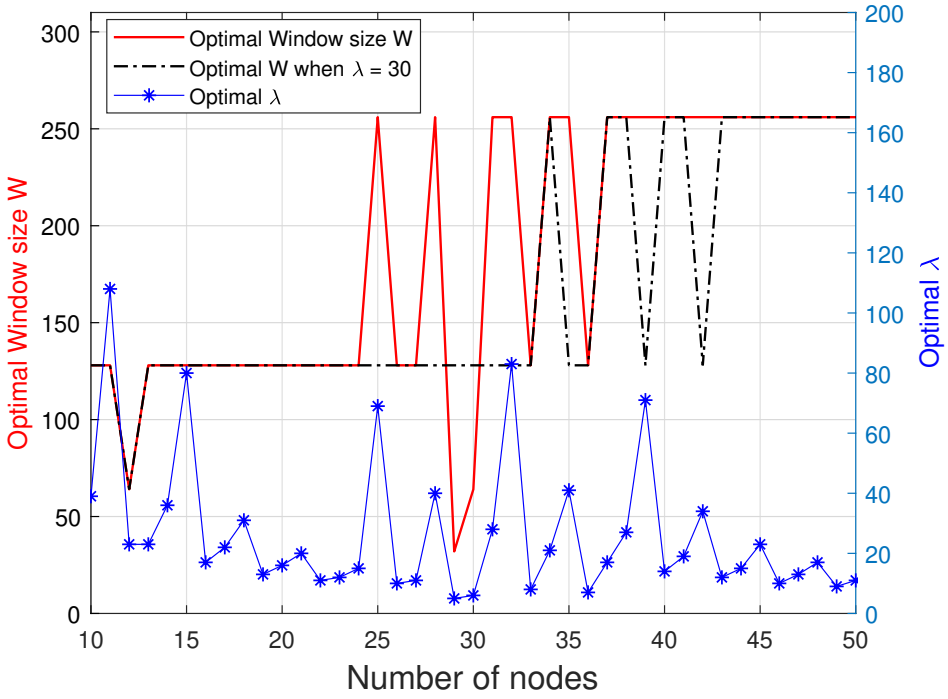

Figure 3.14: Optimal pairs for W and λ under different number of nodes and optimal W for $\lambda = 30$

worth noting that it is sub-optimal. When λ is fixed, the corresponding value of W escalates with the node number growing, so most of the time, the value of W falls between two window sizes. In this case, the window size that can be used to get a higher P_s is selected. Hence, according to the result, when designing the wireless PBFT network, the optimal W are mostly 128 and 256, depending on the network scale. Nevertheless, bigger contention window sizes also make a node wait more time on average to initiate a transmission, thus incurring more delay. The trade-off between throughput and delay is worth considering.

3.7 Conclusion

This chapter provides the performance evaluation of traditional PBFT over the IEEE 802.11 wireless network. It investigates the impacts of channel contention and the view change on wireless PBFT networks. Moreover, the optimal configurations of contention window size and packet arrival rate for different network sizes are obtained, where the optimal W can be chosen for the best network performance, with known n and λ. The results have proven that the influence on the view change delay from channel contention is slight, while the latter will significantly reduce the success probability of the PBFT network.

Hence, a dedicated wireless network is essential for PBFT implementation. The chapter further demonstrates the optimal pairs of the W and λ which provides straightforward guidance for future wireless PBFT networks. In particular, the results show the ideal contention window sizes are 128 and 256 when the network size is small (up to 50 nodes).

The performance of the wireless PBFT network will be greatly impaired due to the attributes of the wireless network. Hence, an improved PBFT designed for the wireless network needs to be researched. In the future, a retransmission mechanism that may improve the success probability of a consensus round is worth investigating. However, this may require more time to complete a consensus process. Thus, the trade-off between the success probability and delay is worth investigating. Moreover, a scenario where an adaptive PBFT network is implemented in a cellular network is also worth exploring. Usually, energy consumption is an important performance indicator of the wireless network. Especially the IEEE 802.11 broadcast scheme is a short-range protocol commonly referred to as WiFi that consumes a relatively large amount of energy. This can be a bottleneck for the IoT network, where most devices are battery-powered and have limited capacity. Therefore, measuring the energy consumption of the wireless blockchain network is a good indicator of sustainability.

Chapter 4

Base Station Enabled Wireless PBFT Network

In the previous chapter, the PBFT protocol was implemented with the IEEE 802.11 broadcast scheme under an unsaturated scenario, which achieves high consensus success probability, high throughput, and low latency when the network size is small. However, the probability of collisions increases sharply as the network size increases, greatly impairing the effectiveness and scalability of the PBFT network. In addition, due to the transmission range of mobile devices, the connectivity and choice of accessible devices have become more restricted. This chapter focuses on the wireless PBFT network enabled by the base station, where inter-node communication is achieved through the base stations. Under the conventional structure of the PBFT, the communication complexity increases drastically as the number of nodes increases. To tackle this problem, a novel 'timeout' mechanism is proposed, where the base stations aggregate the messages and further forward them to the destinations. The key performance indicators of the base station-enabled wireless PBFT network are consensus success probability, communication complexity, view change delay, view change occurrence probability, average transmit power, consensus delay and consensus throughput. The numerical results demonstrate that compared to the wireless PBFT network using IEEE 802.11, the base station-enabled wireless PBFT network provides a broader connection, a higher communication success rate and higher network scalability and accessibility. A special case with f deterministic byzantine nodes is also investigated, proving that prior knowledge of the byzantine nodes can increase the consensus success probability. Moreover, the optimal configurations of the network parameter for achieving the desired

consensus success probability are analysed and derived.

4.1 Introduction

Voting-based blockchains such as PBFT are feasible for the next-generation networks to embrace. PBFT was developed from the byzantine fault tolerance [111]. Compared with Paxos and Raft, the trait of PBFT that it can tolerate up to $\lfloor \frac{n-1}{3} \rfloor$ faulty or non-responsive nodes of the total n nodes in the network makes it stand out since in the wireless environment, the transmitted packets could get lost or compromised due to collisions, blockages or interference. In such a case, the PBFT can discard those lost nodes as faulty or non-responding nodes and perform normally. In contrast to the mining-based ones, voting-based blockchains reach consensus through inter-participant communications, requiring nearly zero computation while offering much higher throughput and low latency. However, the effectiveness of voting-based wireless blockchains is heavily influenced by the quality of the wireless channel, as the consensus mechanism relies significantly on inter-participant communication. Furthermore, the substantial communication overhead implies that voting-based blockchains are only suitable for small-scale networks [112]. Nevertheless, in addition to the inherent security and distributed features of blockchain and the scalability and low latency provided by the voting-based blockchain, PBFT can offer essential byzantine faults tolerance and resilience in the wireless network, where nodes are susceptible to various failures or malicious attacks, and the environments are highly dynamic and unpredictable [113].

The performance of the wireless PBFT network using IEEE 802.11 broadcast scheme is restrained a lot by the wireless protocol (i.e. the transmission success probability is greatly reduced when the network size scales up), hence resulting in a lower scalable use case. Initially, consensus mechanisms are designed for wired networks, where the link is reliable and stable, but wireless networks can offer greater accessibility and a larger pool of available nodes. The inherent limitations of PBFT in terms of scalability have restricted its feasibility for large-scale deployment in wireless networks.

This chapter proposes a novel framework for implementing the PBFT protocol over the wireless cellular network to address these challenges, aiming to enhance node accessibility and scalability significantly. The wireless cellular network is assumed to be operated by a single class of base stations (i.e. macro base stations). Nodes are served by the base station, and the inter-node communications entirely

rely on the base stations. Consequently, the coverage of the base stations determines the probability that a random node can correctly decode the received signal, which further impacts the consensus success rate of the PBFT. The Poisson point process (PPP) on a 2-D plane is used to model the distribution of the base stations and nodes. In the cellular PBFT network, it is considered the uplink and downlink communications between the PBFT nodes and the base station to be susceptible to failures because of the outage area to each other. Therefore, both the uplink and downlink communication success probabilities are analytically derived based on the coverage probability. Through analysis and simulation results, the introduction of the base station in the PBFT benefits from the following aspects:

- Large range: With base stations facilitating normal operations, more connected nodes can potentially participate in the PBFT network.
- Scalability: The simulation results show that as long as the uplink and downlink success probabilities are high, the PBFT consensus success probability may increase as more nodes join the consensus network.
- Latency: The base station provides dedicated resources for PBFT nodes, eliminating the need for carrier sense and reducing packet loss due to collisions in ad hoc networks. This allows multiple uplink and downlink communications to occur simultaneously, resulting in lower latency.
- Communication complexity: The *timeout* mechanism at the base station that aggregates the messages and broadcasts them substantially reduces the communication complexity. This trait also contributes to scalability.
- Throughput: Thanks to the low complexity and latency, the framework achieves a better throughput compared to the conventional PBFT network.

4.2 System Model

4.2.1 Practical Byzantine Fault Tolerance in Cellular Networks

This subsection focuses on how PBFT is implemented in the cellular network.

PBFT is a voting-based blockchain consensus algorithm famous for its fault-tolerant characteristic. The nodes comprising the PBFT network are called

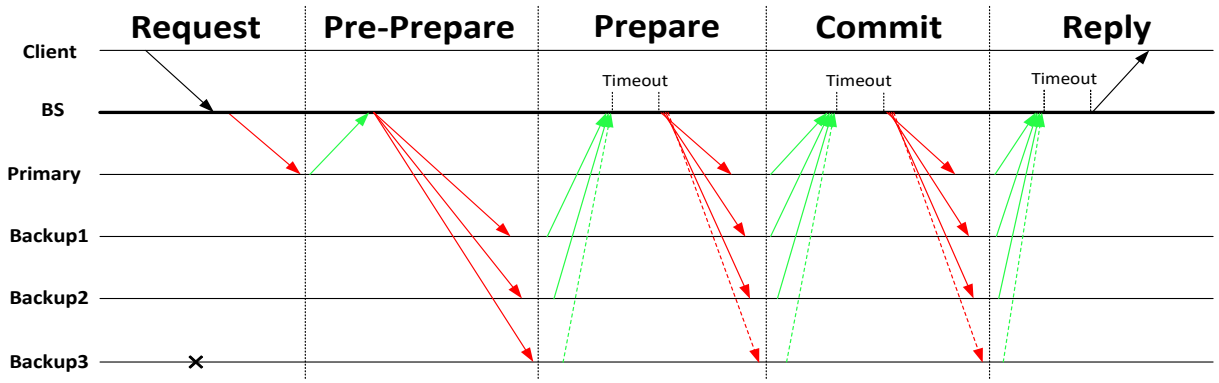

Figure 4.1: The normal case operation of PBFT in the cellular network

replicas. A PBFT network with n replicas can tolerate up to f faulty nodes, and the relation between n and f satisfies

$$f \leq \left\lfloor \frac{n-1}{3} \right\rfloor. \tag{4.1}$$

A PBFT network comprises two types of nodes: a primary and backups, as shown in Fig. 2.1. The primary is selected following a round-robin pattern, which means every node has an equal probability of serving as a primary. The time span of a primary is called a view. Hence, each view has only one primary. The initialization of primary selection is guided by the view change mechanism, which guarantees the liveness of the PBFT network. The view change mechanism is triggered to select a new primary whenever the current primary fails, and the PBFT system enters a new view. Let R denote the set of the PBFT nodes, and v denote the view, and the new primary node p in the v^{th} view is such that $p = v \bmod |R|$.

A timeout mechanism at the base station to optimize the communication complexity is introduced, which is a gap between the base stations receiving and transmitting the messages, as shown in Fig. 4.1. A processing *timeout* is set up when the base stations receive broadcast requests from the nodes in the *prepare*, *commit* and *reply* phase with the same view number. During the *timeout*, the base stations generate an aggregated message with the transmitting nodes' identity sequence number in $\{0, ..., |R| - 1\}$. After the *timeout*, the base station stops aggregating and broadcasts the aggregated message to the nodes, and any message received with the view number for the previous *timeouts* will be discarded. In the *reply* phase, the base station aggregates the message from the backups to the client. How the value of the *timeout* is determined will be discussed in section 4.3.4.

The consensus of PBFT is achieved following a process called normal case operation. The primary broadcasts the client's request to all the backups for execution, as shown in Fig. 2.1. However, in the cellular network environment, the inter-node communications must go through the base stations, as shown in Fig 4.1. The normal case operation in the cellular PBFT network follows:

- PRE-PREPARE: After receiving the request from the client forwarded by the base stations, the primary sends the *pre-prepare* message to the base station, which further broadcasts the *pre-prepare* message to every node.
- PREPARE: All backups transmit the *prepare* message to the base stations, and the base station aggregates the message and broadcasts the *prepare* message to all nodes. The backups only proceed to the *commit* phase when they receive the *prepare* message with at least $2f$ matched view and identity numbers.
- COMMIT: Every nodes transmits and receives the *commit* message through the base stations. Similarly, the backups only proceed to the next phase when they receive the *commit* message with at least $2f + 1$ matched view and identity numbers.
- REPLY: All nodes forward the *reply* message to the client through the base stations.

The client only admits the validity of the consensus to the request when the *reply* message contains at least $2f+1$ identity numbers and matched views. PBFT can tolerate up to f byzantine nodes, which are malicious (send adverse responses to subvert the consensus). In the worst case where f good nodes are non-responding and all f byzantine are involved in the consensus process, at least $f+1$ messages from the good nodes (hence $2f+1$ in total) is the minimum requirement to ensure the validity of the consensus.

4.2.2 Downlink and Uplink Communications

This chapter considers that the cellular network is composed of a single class of base stations and nodes in the Euclidean plane [114] and orthogonal multiple access (OMA) is incorporated. It is assumed that only one node is active in a cell per time slot. Hence, the active nodes and base stations are considered independently distributed according to the PPP with the same intensity λ and nodes always associate with the nearest base station for received power maximization [115]. Hence, a Voronoi tessellation on the plane is formed where

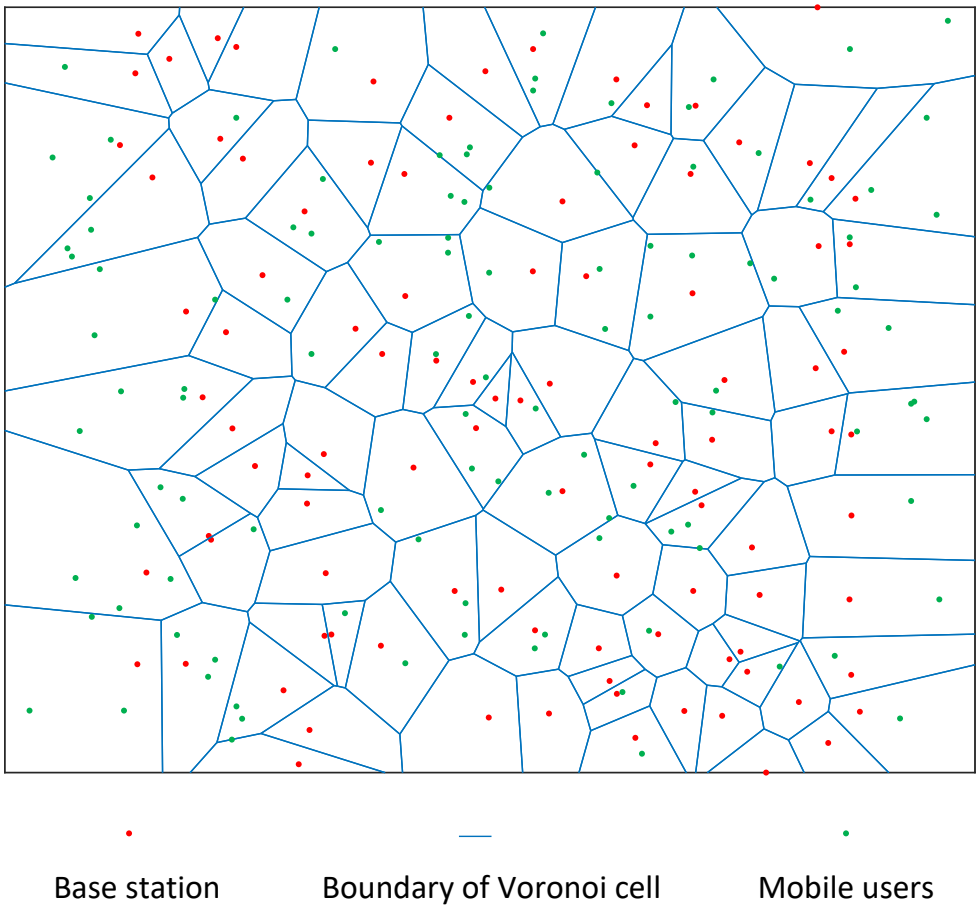

Figure 4.2: The Voronoi of Poisson distributed base stations and mobiles

exactly one base station falls in one Voronoi cell, as shown in Fig. 4.2.

Assume that the distance from a base station to its nearest node is r; hence, no other base station to the particular node should be closer than r.

Theorem 5. *The probability density function (PDF) of r, the distance between a base station and its nearest node, can be expressed as follows [115]*

$$f(r) = 2\pi\lambda r e^{-\lambda\pi r^2}, r > 0. \tag{4.2}$$

Fig 4.3 demonstrates the diagram of the inter-node communication among nodes through the base station in the *pre-prepare* phase. This process corresponds to the workflow shown in Figure 4.1 and the architecture depicted in Figure 4.2. In this phase, the primary node sends the *pre-prepare* message to the base stations interconnected via the X2 interface. The base stations then forward the *pre-prepare* message to the backup nodes. Following this, the normal operation proceeds as outlined in Section 4.2.1.

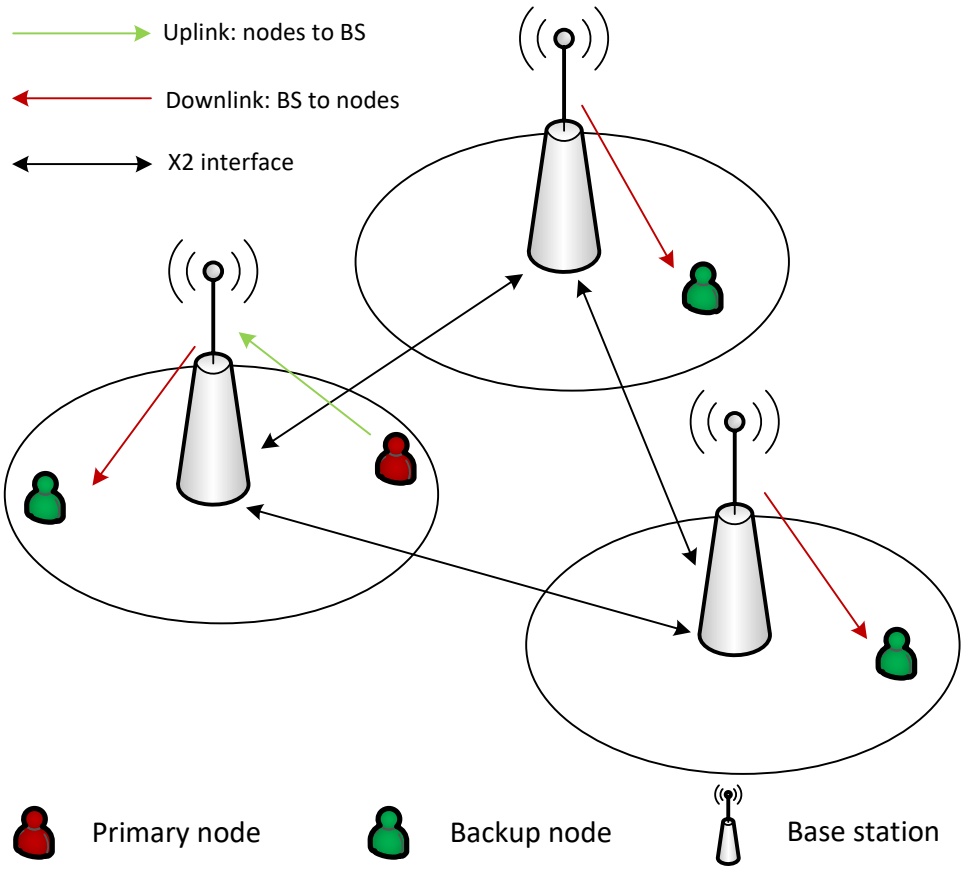

Figure 4.3: The diagram of the cellular PBFT network

4.2.3 Channel model

In this model, the channel experiences the path loss with a path loss exponent denoted by α and the path loss is assumed to be inversely proportional to the distance. It is assumed that the link between base stations and nodes experiences Rayleigh fading with a mean of 1.

In the downlink communication, if the distance between a node and its serving BS is r and the base stations have a constant transmit power of u_b^{-1}, then the received power by the node is $G_{bm}r^{-\alpha}$, where G_{bm} is the channel gain following an i.i.d exponentially distribution with a mean of u_b^{-1} as $G_{bm} \sim \exp(\mu_b)$. The noise power is assumed to be constant at σ^2. For the downlink communication, the SINR at a node is expressed as

$$\text{SINR}_{DL} = \frac{G_{bm}r^{-\alpha}}{\sigma^2 + I_{\mathcal{Z}_b}}, \tag{4.3}$$

where $I_{\mathcal{Z}_b}$ is interference from the interfering set of base stations denoted by $\mathcal{Z}_b$,

and it follows,

$$I_{\mathcal{Z}_b} = \sum_{i \in \Phi, \mathcal{Z}_b} G_i R_i^{-\alpha}, \tag{4.4}$$

where the particular base station i of $\mathcal{Z}_b$ is at a distance of R_i and have a channel gain G_i.
The uplink SINR at a base station is expressed as

$$\text{SINR}_{UL} = \frac{G_{mb} r^{-\alpha}}{\sigma^2 + I_{\mathcal{Z}_m}}, \tag{4.5}$$

where G_{mb} is the channel gain between the tagged base station and node, and it follows an i.i.d exponentially distribution with a mean of u_m^{-1} as $G_m \sim \exp(\mu_m)$. $I_{\mathcal{Z}_m}$ is interference from the interfering set of nodes denoted by $\mathcal{Z}_m$, and it follows,

$$I_{\mathcal{Z}_m} = \sum_{j \in \Phi, \mathcal{Z}_m} G_j R_j^{-\alpha}, \tag{4.6}$$

where the particular node j of $\mathcal{Z}_m$ is at a distance of R_j and have a channel gain G_j.

4.2.4 Coverage Probability

The coverage probability plays a huge role in the consensus success probability, as the consensus is reached relying on substantial inter-node communications in the PBFT network. In our framework, the consensus relies on the communications between the nodes and base stations. It is assumed that the nodes and base stations are in each other's coverage when their SINR is beyond the threshold T. They are considered in the outage area when their SINR is below T. Hence, the coverage probability of the nodes and base stations can be defined by the complementary cumulative distribution function (CCDF) [116] as

$$P = \mathbb{P}[\text{SINR} > T]. \tag{4.7}$$

Theorem 6. *The coverage probabilities of the nodes and base stations can be finalised as [114]*

$$P(T, \lambda, \alpha) = \int_{r>0} 2\pi\lambda r e^{\pi\lambda r^2 \mu T r^\alpha \sigma^2} \mathcal{L}_{Ir}(\mu T r^\alpha), \tag{4.8}$$

where

$$\mathcal{L}_{I_{\mathcal{Z}}}(\mu T r^{\alpha}) = \exp\left(-\lambda \int_{r}^{\infty} \left(1 - \int_{0}^{\infty} e^{-\mu T r^{\alpha} g v^{-\alpha}} f(g)\, dg\right) dv\right),$$

and $f(g)$ is from (4.2).

4.3 Performance Analysis of the BS-enabled PBFT network

This section focuses on the performance analysis of the BS-enabled PBFT network. Particularly, this section presents the success probability at each of the phases of the BS-enabled PBFT consensus network and its end-to-end success probability. A special case of how f deterministic byzantine nodes in the network influence the consensus success probability is discussed. In addition, the communication complexity and the average transmit power are analytically derived and compared with the conventional PBFT network. View change delay and occurrence probability are analytically derived, which measure the resilience of the PBFT network. Furthermore, the consensus delay and throughput are presented.

4.3.1 Consensus Success Probability

Consensus success probability is an important performance indicator of a consensus mechanism of blockchain. In the wireless scenario, the consensus success probability is influenced a lot by packet loss, collisions, or outages due to the nature of the wireless channel. Even worse, the consensus can be tempered with the presence of the byzantine nodes in the wireless environment. This section presents the coverage probabilities of the nodes and base stations and derives the consensus success probability based on the coverage probabilities. A special case where there are f deterministic byzantine nodes is also discussed.

The consensus is reached through the normal case operation and confirmed valid by the number of replies received by the client. The consensus success probability is significantly reliant on the coverage probability. In the normal case, it is assumed there are up to f byzantine nodes in the PBFT network, and all the failures are due to the communication outage.

Pre-prepare Phase Success Probability

In the *pre-prepare* phase of the cellular PBFT networks, a consensus request is initiated by a client to the primary through the base station. For tractability, it is assumed that the connection between the primary and client is 100% stable. Once the primary receives the request, it broadcasts the *pre-prepare* message to all replicas through the base station with a success probability of P_{ul}, where P_{ul} is uplink transmission success probability and obtained from (4.8) by substituting the SINR threshold of PBFT nodes T_m. The base station then further broadcasts the *pre-prepare* message to all replicas. Note that even though there is no restriction on the number of received *pre-prepare* messages in this phase, no more than f nodes fail to receive the *pre-prepare* message to ensure enough *prepare* messages can be transmitted in the next phase. Therefore, the *pre-prepare* phase success probability is given by

$$P_{pre-prepare} = P_{ul} \sum_{i=0}^{f} \binom{n-1}{i} {P_{dl}}^{n-1-i} (1 - P_{dl})^{i}, \tag{4.9}$$

where P_{dl} is the downlink success probability from the base to the PBFT nodes and is obtained from (4.8).

Prepare Phase Success Probability

All nodes with the exception of the primary node enter the *prepare* phase after receiving the *pre-prepare* messages, and broadcast the *prepare* message to the other replicas through the base station. A node verifies the *prepare* message by checking if it receives more than $2f$ prepare messages from different nodes. Once the validity of the *prepare* message is confirmed, nodes can proceed to the *commit* phase. The whole process of the *prepare* phase can be divided into uplink and downlink communication. In the uplink communication, at least $2f$ nodes need to broadcast the *prepare* message to confirm its validity, and the success probability of the uplink communication can be expressed as

$$P_{prepare}^{UP} = \sum_{j_1=2f}^{n-1} \binom{n-1-i}{j_1} {P_{ul}}^{j_1} (1 - P_{ul})^{n-1-i-j_1}. \tag{4.10}$$

In the normal case of conventional PBFT, the primary is not involved in the *prepare* phase, so it only requires every backup node to receive at least $2f$ *prepare* message for validity. In the downlink communication of the cellular PBFT network, even though the validity of the *prepare* message can be confirmed by

$2f$ different signatures, at least $2f + 1$ nodes, including the primary, have to receive the aggregated message to make sure enough nodes can proceed to the next phase. Therefore, the success probability of the downlink communication is given by

$$P_{prepare}^{DN} = \sum_{j_2=2f+1}^{n} \binom{n}{j_2} {P_{dl}}^{j_2} (1 - P_{dl})^{n-j_2}. \tag{4.11}$$

The overall success probability of the *prepare* phase is given by

$$P_{prepare} = P_{prepare}^{UP} \cdot P_{prepare}^{DN}. \tag{4.12}$$

Commit Phase Success Probability

Similar to the *prepare* phase with a minor difference where the primary is involved in this phase, *commit* phase requires each nodes to receive at least $2f+1$ *commit* messages from different nodes. In the uplink communication, at least $2f + 1$ nodes send the *commit* message to the base station. The success probability of the uplink communication is given by

$$P_{commit}^{UP} = \sum_{m_1=2f+1}^{n} \binom{n - j_2}{m_1} {P_{ul}}^{m_1} (1 - P_{ul})^{n-j_2-m_1}. \tag{4.13}$$

In the downlink communication, as the *commit* message is verified with $2f + 1$ different sources, the success probability of the downlink communication is calculated by

$$P_{commit}^{DN} = \sum_{m_2=2f+1}^{n} \binom{n}{m_2} {P_{dl}}^{m_2} (1 - P_{dl})^{n-m_2}. \tag{4.14}$$

The success probability of the *commit* phase is given by

$$P_{commit} = P_{commit}^{UP} \cdot P_{commit}^{DN}. \tag{4.15}$$

End-to-end Success Probability

To qualify a successful consensus, it must go through the whole normal case operation from the *pre-prepare* to the *commit* phase. Hence, the end-to-end success probability of the cellular PBFT network can be obtained by

$$P_{consensus} = P_{pre-prepare} \cdot P_{prepare} \cdot P_{commit}, \tag{4.16}$$

where $P_{pre-prepare}$, $P_{prepare}$ and P_{commit} are given in (4.9), (4.12) and (4.15), respectively.

4.3.2 Special case: f deterministic Byzantine nodes

In the previous parts, the nodes in the PBFT network are all assumed to have up to f byzantine nodes, but the exact number is not defined, and all the failures are due to communication outages. This subsection investigates the safety of the PBFT in the cellular network with f deterministic byzantine nodes.

It is assumed that the byzantine nodes always send negative messages to tamper with the result of the consensus, while the honest nodes always send positive messages. The byzantine nodes are assumed to share the attributes of the other nodes, which also suffer from the outage. In the normal case, to reach a valid consensus, two conditions should be fulfilled:

- The client receives a minimum of $2f + 1$ replies due to the timeout mechanism to ensure at least $f + 1$ matching replies.
- The number of replies from the honest nodes is more than that of the byzantine nodes.

In the normal case of PBFT, where the number of byzantine nodes is arbitrary but limited up to f, the minimum number of replies received by the client to confirm a valid consensus is $2f + 1$. Let M_r denote the number of total replies received by the client, M_h denote the number of replies received by the client from the honest nodes, and M_b denote the number of replies received by the client from the byzantine nodes. Therefore, the consensus success probability of the PBFT network can be defined by the CCDF as

$$\overline{P}_{con} = \mathbb{P}[M_r >= 2f + 1, M_h > M_b]. \tag{4.17}$$

However, in the PBFT network with f deterministic byzantine nodes, a valid consensus can be formed when the client receives at least $f + 1$ replies from the honest nodes. Therefore, (4.17) can be written as

$$\overline{P}_{con} = \mathbb{P}[M_h > f + 1]. \tag{4.18}$$

For tractability, for this special case, we use a general inter-node communication success probability P_s and assume that the primary is not byzantine.

Theorem 7. *The final expression of each phases' consensus success probability of the PBFT cellular network with f deterministic byzantine nodes out of $n = 3f+1$*

total nodes can be expressed as

$$\overline{P}_{con} = \sum_{i=f}^{2f} \sum_{m=f+1}^{2f+1} \binom{2f}{i} \binom{2f+1}{m} {P_s}^{m+i} (1-P_s)^{4f+1-i-m}. \tag{4.19}$$

Proof. In the network with f deterministic byzantine nodes and $2f+1$ honest nodes, at least $f+1$ honest nodes must be involved in the consensus process. It is assumed that the primary is honest and can achieve 100% success in the *pre-prepare* phase (every backup can receive the *pre-prepare* message).

In the *pre-prepare* phase, backup nodes send the *pre-prepare* message to the others, and the primary only receives the *pre-prepare* message. Therefore, at least f out of $2f$ honest nodes must successfully transmit the *pre-prepare* message. The success probability of the *pre-prepare* phase for PBFT with f deterministic nodes is given by

$$\sum_{i=f}^{2f} \binom{2f}{i} {P_s}^{i} (1-P_s)^{2f-i}. \tag{4.20}$$

□

In the *commit* phase, every node, including the primary, has to send the *commit* message. Hence, at least $f+1$ out of $2f+1$ honest nodes must successfully transmit the *commit* message. The success probability of the *commit* phase for PBFT with f deterministic nodes is given by

$$\sum_{m=f+1}^{2f+1} \binom{2f+1}{m} {P_s}^{m} (1-P_s)^{2f+1-m}. \tag{4.21}$$

By multiplying (4.20) and (4.21), (4.19) is therefore reached.

4.3.3 Communication Complexity

This section presents the communication complexity analysis of the conventional PBFT consensus network and PBFT in the cellular network. All the complexity analysis is conducted at the premise of the ideal condition where all the transmissions are successful.

Communication Complexity of PBFT

PBFT reaches consensus by the normal case operation [73] through four stages: *pre-prepare*, *prepare*, *commit*, and *reply*, as shown in Fig. 2.1. The normal

case operation requires massive inter-node communications to execute the request initiated by a client before a consensus is achieved. Let C denote the communication complexity of PBFT, which is composed of four parts. That is, the complexities of the 1) *pre-prepare* phase, C_{pp}, 2) *prepare* phase, C_p, 3) *commit* phase, C_c, and 4) *reply* phase, C_r. Therefore,

$$C = C_{pp} + C_p + C_c + C_r. \tag{4.22}$$

After receiving the request from the client to the primary, the PBFT network begins a normal case operation. Provide that the PBFT network has n nodes. In the *pre-prepare* phase, the primary broadcasts a *pre-prepare* message to the rest of the nodes. Hence,

$$C_{pp} = n - 1. \tag{4.23}$$

In the *prepare* phase, every node apart from the primary broadcasts a *prepare* message to the other nodes. Then

$$C_p = (n-1)^2. \tag{4.24}$$

In the *commit* phase, every node broadcasts a *commit* message to the other nodes. Thus,

$$C_c = n \cdot (n-1). \tag{4.25}$$

Finally, every node returns the outcome to the client in the *reply* phase. We can obtain

$$C_r = n. \tag{4.26}$$

Based on (4.23) to (4.26), the PBFT's complexity in (4.22) can be expressed as follows

$$C = 2n^2 - n. \tag{4.27}$$

Communication Complexity of Cellular PBFT Network

In the cellular PBFT network with n nodes, every inter-node communication goes through base stations. Let $\overline{C}$ denote the communication complexity of PBFT in the cellular network, which also consists of four components: the complexities of the 1) *pre-prepare* phase, $\overline{C}_{pp}$, 2) *prepare* phase, $\overline{C}_p$, 3) *commit* phase, $\overline{C}_c$, and 4) *reply* phase, $\overline{C}_r$.

As indicated in Fig. 4.1, there is only one uplink communication from the primary to the base station, whereas in the downlink communication, the base station broadcasts the *pre-prepare* message to all backups. Therefore, the *pre-prepare*

phase of the PBFT in a cellular network involves a communication complexity of $\overline{C}_{pp} = n$.

Further, in the *prepare* phase, all backups participate the uplink communications, and every node receives the *prepare* from the base station. Hence, this phase has a communication complexity of $\overline{C}_p = 2n - 1$.

In the *commit* phase, every node participates in both uplink and downlink communications. Thus, $\overline{C}_c = 2n$.

In the *reply* phase, the base station forwards the *reply* messages from all the replicas to the client. This process involves $n + 1$ times of communications. Hence, the whole *reply* phase has a communication complexity of $\overline{C}_r = n + 1$.

With the components above, the communication complexity of PBFT in the cellular network can be expressed as

$$\overline{C} = 6n. \tag{4.28}$$

From (4.27) and (4.28), the cellular PBFT network has less communication complexity for any n. In the smallest PBFT network with $n = 4$, $\overline{C} = 24 \leq C = 26$. The advantage of the cellular PBFT network further expands as the network size increases, as the complexity of the PBFT scales quadratically with n while that of the cellular PBFT network scales linearly.

4.3.4 View Change

The view change mechanism guarantees the liveness of the PBFT network by forcing the network into the new view to prevent the whole system from waiting an indefinite time for execution. In the context of wireless networks, the view change mechanism is initiated by a faulty primary due to the nature of the wireless channel. This section focuses on the view change occurrence probability and average view change delay for the networks under different sizes.

View Change Occurrence Probability

The view change mechanism is initiated to select a new functional primary when the last primary becomes faulty and follows a round-robin pattern. Hence, every node in the PBFT system has an equal probability of being a primary. However, since the PBFT system can tolerate up to $\lfloor \frac{n-1}{3} \rfloor$ faulty nodes out of n total nodes, the newly selected primary can possibly still be a faulty node. In such a case, the view change mechanism carries on until a good primary is selected. Therefore, the view change occurrence probability is introduced to measure the likelihood that the view change mechanism remains on after a primary is selected.

It is considered that in the cellular PBFT, the failure of the primary is due to the failed uplink communication in the *pre-prepare* phase. A primary is assumed to be faulty when it is in the outage area of base stations. Hence, the probability of a primary failure is given by

$$P_f = 1 - P_{ul}. \tag{4.29}$$

Every node is assumed to have the same downlink and uplink success probability from and to the base stations. Hence, the identical node failure probability P_f applies to every node in the PBFT network. To reach a successful consensus, a PBFT network can only tolerate up to $\lfloor \frac{n-1}{3} \rfloor$ faulty nodes. Let P_{f_i} denote the probability of the case where there are i faulty nodes in the PBFT network, and it can be expressed as

$$P_{f_i} = \binom{n}{i} {P_f}^i (1 - P_f)^{n-i}. \tag{4.30}$$

Since the view change mechanism is performed by the round-robin scheme, every node has an equal probability of being selected as the next primary. In the case of i faulty nodes in the PBFT network, when a new primary node is selected, it has a $\frac{i}{n}$ probability of being faulty and triggering the view change mechanism. Hence, the conditional probability of view change occurrence in a PBFT network with n nodes and i faulty nodes is given by

$$P_{vc}(n|f = i) = P_{f_i} \frac{i}{n}. \tag{4.31}$$

By summing up every possible case, the average view change occurrence probability for a PBFT network with n nodes is therefore obtained as

$$P_{vc} = \sum_{i=1}^{\lfloor \frac{n-1}{3} \rfloor} P_{f_i} \frac{i}{n}. \tag{4.32}$$

Average View Change Delay

The view change mechanism provides liveness to the PBFT network. The view change delay refers to the duration from when the view change mechanism is initiated to when a primary is selected. The view change delay measures how resilient the PBFT system is from a failure. A view change is triggered by timeouts. Every node has a view change timer, which starts when the node receives a request and stops when the request is executed. A new timer is set up when a new request arrives [73]. If the timer is up before the request is executed,

a node broadcasts the view change message to the others. A node enters a new view by receiving at least $2f$ valid view change messages.

Theorem 8. *The expression of the average view change delay of the network with n nodes is given in (4.33), where the $\overline{D_e}$ is the transaction delay for each round of consensus, the ζ is the view change timeout, and P_{f_i} is the probability of i faulty nodes defined in (4.30).*

$$D_{vc}(n) = \begin{cases} P_{f_1}(\overline{D_e} + \frac{1}{n-1}(\zeta + \overline{D_e})) & n < 7 \\ P_{f_1}(\overline{D_e} + \frac{1}{n-1}(\zeta + \overline{D_e})) + \sum_{m=2}^{\lfloor \frac{n-1}{3} \rfloor} P_{f_m}\Big(\frac{n-m}{n-1}\overline{D_e} + \frac{m}{n-1} & \\ \Big((\frac{n-m}{n-2})(\zeta + \overline{D_e}) + \sum_{i=2}^{m} [i \cdot \zeta + \overline{D_e}] \frac{n-m}{n-1-i} \prod_{v=1}^{i-1} (\frac{m-v}{n-1-v}) \Big) \Big) & n >= 7 \end{cases} \tag{4.33}$$

Proof. The maximum number of faulty nodes in the wireless cellular PBFT network with n nodes is $\lfloor \frac{n-1}{3} \rfloor$. It is important to note that the view change mechanism is only effective when the number of faulty nodes is below a certain threshold. Therefore, there is P_{f_1} probability of there being only 1 faulty node in such a network. In this case, when a primary fails, the next primary has $\frac{1}{n-1}$ probability of being faulty. Hence, the view change delay in the case where there is only 1 faulty node is given by

$$P_{f_1}(\overline{D_e} + \frac{1}{n-1}(\zeta + \overline{D_e})), \tag{4.34}$$

as shown in the upper part of (3.25).
With the network's scale growing, the PBFT network is able to tolerate more faulty nodes (when $n \geq 7$, $f \geq 2$). As the case with 1 faulty node is the same as above, we carry on with the case with 2 faulty nodes and above. The probability that the network has exact 2 faulty nodes is P_{f_2}. It might take one or two extra selections to exhaust the faulty nodes, so the view change delay for this case is given by

$$P_{f_2}\Big(\frac{n-2}{n-1}\overline{D_e} + \frac{2}{n-1}\Big((\zeta + \overline{D_e}) + \frac{1}{n-2}(2\zeta + \overline{D_e}) \Big) \Big). \tag{4.35}$$

By summing up such two conditional probabilities, the average view change delay for the network, which can tolerate 2 faulty nodes, is obtained as

$$\begin{aligned} D_{vc}(n|f=2) = P_{f_1}(\overline{D_e} + \frac{1}{n-1}(\zeta + \overline{D_e})) + P_{f_2}\Big(\frac{n-2}{n-1}\overline{D_e} \\ + \frac{2}{n-1}\Big((\zeta + \overline{D_e}) + \frac{1}{n-2}(2\zeta + \overline{D_e}) \Big) \Big). \end{aligned} \tag{4.36}$$

Likewise, the lower part of (3.25) is therefore deduced in a similar way. □

4.3.5 Consensus Delay and Throughput

It takes some time to reach a consensus in the PBFT, and the time taken for a consensus agreement is defined as the consensus delay. The consensus throughput is the number of the consensus reached over a unit of time. This section discusses the consensus delay and throughput as well as their derivations.

In the BS-enabled wireless PBFT framework, the delay is assumed to consist of two components: the timeout at the base station and the communication delay in the consensus process. In general, the communication delay is mainly from four parts: propagation, processing, transmission, and queuing delays [117]. The propagation delay is the time needed to propagate a packet on a medium between the nodes and base stations. The processing delay refers to when the base station and nodes's routers need to process the packet header to direct the packets to their destinations. However, such two delays are negligibly small in our framework. Hence, we only consider transmission and queuing delays.

The transmission delay refers to the time required for a transmitter to push the packet to the communication link. The queuing delay is the time a packet needs to wait in the buffer before it is pushed to the link. Suppose packets arrive at the system at a rate of $\overline{\lambda}$ with a length of L bits, and the transmission rate of a base station is $\overline{\mu}$. The arrival and transmission rates follow Poisson and Exponential distribution [118]. Hence, the network utilization rate can be calculated as

$$\rho = \frac{\overline{\lambda} L}{\overline{\mu}}. \tag{4.37}$$

Besides, the transmission delay for a packet can be obtained as

$$D_{trans} = \frac{L}{\overline{\mu}}. \tag{4.38}$$

According to Little's law [119], the number of packets in the system is given by

$$S = \frac{\rho}{1-\rho} = \frac{\overline{\lambda} L}{\overline{\mu} - \overline{\lambda} L}. \tag{4.39}$$

Furthermore, the average number of packets in the queue is given by

$$Q = S \cdot \rho = \frac{\rho^2}{1-\rho}. \tag{4.40}$$

The average queuing delay is therefore given by

$$D_{que} = \frac{Q}{\overline{\lambda}} = \frac{\rho}{\overline{\mu} - \overline{\lambda}L}. \tag{4.41}$$

The total delay can be expressed as

$$D = D_{trans} + D_{que} = \frac{1}{\overline{\mu} - \overline{\lambda}L}. \tag{4.42}$$

As the majority of the communications are offloaded to the base stations, we only consider the delay that occurred in the base station. It is assumed that a *timeout* that equals the total delay D of a consensus is enough. According to Fig. 4.1, *timeout* happens three times during a consensus process. Hence, there are 4 base station broadcasts and three *timeouts* involved in a consensus process. Hereby, the consensus delay can be expressed as

$$D_{con} \approx 4D + 3 \cdot timeout = \frac{7}{\overline{\mu} - \overline{\lambda}L}. \tag{4.43}$$

As the consensus throughput is the number of consensus reached over a unit of time, it is obtained as the inverse of the consensus delay

$$R = \frac{1}{D_{con}}. \tag{4.44}$$

4.3.6 Energy Consumption

Energy Consumption is an important key performance indicator that measures the energy consumed during the consensus process. This indicates the network's sustainability and efficiency. Suppose that the average packets arrive at a node at a rate $\overline{\lambda}_m$ with a length of L bits, and the transmission rate of a node is $\overline{\mu}_m$. Therefore, the transmission delay of a packet for a node is

$$\overline{D}_{trans} = \frac{L}{\overline{\mu}_m}. \tag{4.45}$$

Suppose that the transmission power of the nodes is denoted as P_{trans}. The energy consumed by a node to transmit a packet can be calculated by the product of transmit power and transmit delay as

$$E_{trans} = P_{trans} \cdot \overline{D}_{trans}. \tag{4.46}$$

In terms of the entire system, energy consumption is the sum of the packets transmitted multiplied by E_{trans}, and it can be expressed as

$$\overline{E}_{total} = E_{trans} \cdot \overline{C}, \tag{4.47}$$

where $\overline{C}$ is given in (4.28).

Provided the same parameters for the conventional PBFT network, the total energy consumption of the conventional PBFT network for reaching a consensus is given by

$$E_{total} = E_{trans} \cdot C, \tag{4.48}$$

where C is given in (4.27).

4.3.7 Average Transmit Power

As the consensus of PBFT relies on inter-node communications, investigating the minimum required transmit power is crucial, for the sake of energy efficiency. We assume that the receiver is equipped with an omnidirectional antenna and can successfully receive a signal when the received power is greater than its sensitivity γ, and the communication follows free-space path loss. In the following, we derive the average transmit power for the conventional wireless PBFT and the BS-enabled wireless PBFT networks.

In the conventional PBFT network, all nodes communicate with each other directly. Hence, they play both the roles of transmitter and receiver. Assume that all nodes have the same sensitivity γ_1, and are distributed in $\mathbb{R}^2$ centered around the primary with a coverage radius R. According to [120], the receiver sensitivity γ is such that

$$\gamma \leq p_t \frac{G_l \lambda^2}{(4\pi d)^2}, \forall d \leq R \tag{4.49}$$

where the G_l is the antenna gain, p_t is the transmit power of the transmitter, λ is the signal wavelength and d is the distance between the transmit and receive antennas. The minimum transmit power p_{min} required by a node at distance $\overline{R}$ from the primary to cover all other nodes in $\mathbb{R}^2$ can be obtained as

$$p_{min} = \frac{\gamma_1}{G_l} \left[\frac{(4\pi \left(\overline{R} + R\right)}{\lambda} \right]^2. \tag{4.50}$$

Furthermore, the average transmit power of the conventional PBFT network is

given by

$$\begin{aligned}\overline{P}_{PBFT} &= \int_0^R p_{min} f(r)\, dr \\ &= \frac{32\pi^2\gamma_1}{G_l\lambda^2}\int_0^{R_1}(R+r)^2\frac{r}{{R_1}^2}\, dr \\ &= \frac{136}{3}\frac{\pi^2\gamma_1}{G_l\lambda^2}R^2.\end{aligned} \tag{4.51}$$

In the BS-enabled PBFT network, the coverage range of the network is determined by the coverage range of the BS in the downlink and the uplink range of the nodes. Assume the sensitivity of the BS is γ_2. The minimum transmitting power of a node at a distance of $\overline{R}$ to the BS located at the origin is given by

$$P_{min}^{BS} = \frac{\gamma_2}{G_l}\left[\frac{(4\pi\overline{R}}{\lambda}\right]^2. \tag{4.52}$$

Consequently, by following the same approach as in (4.51), the average transmit power of nodes in the BS-enabled PBFT network is deduced as

$$\overline{P}_{PBFT}^{BS} = \frac{8\pi^2\gamma_2}{G_l\lambda^2}{R_1}^2. \tag{4.53}$$

It can be seen from the above that the average transmit power of nodes in both the conventional wireless PBFT and the BS-enabled wireless PBFT networks is $\mathbb{O}(R^2)$. However, the coefficient of average transmit power of BS-enabled PBFT network is much lower. Hence, the BS-enabled PBFT network consumes much less power, and this advantage scales up as the network size increases.

4.4 Numerical Results and Discussions

This section presents the numerical results and discussions to underpin the analysis. Moreover, an optimal configuration with different network sizes is analysed and discussed.

Fig. 4.4 shows the uplink and downlink success probability versus different SINR thresholds with the network environment configuration adopted from [114, 115], where $\lambda = 0.25$, $\alpha = 4$ and $\sigma^2 = 0$. The transmit power for the downlink communication is 1 W, whereas the uplink communication has a transmit power of 0.75 W. A good success probability can be achieved when the SINR thresholds are low.

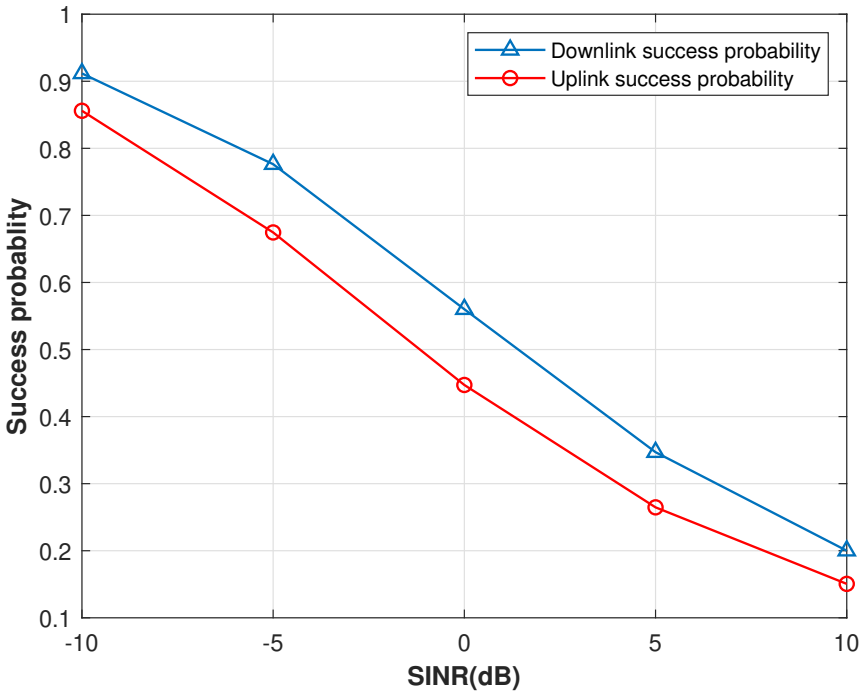

Figure 4.4: Uplink and downlink success probability of versus SINR

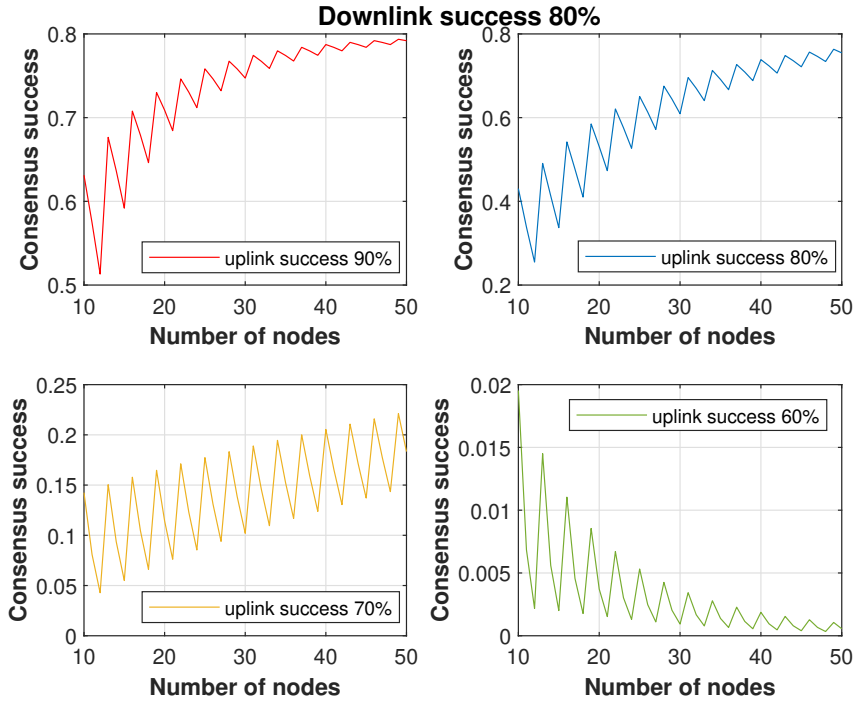

Figure 4.5: Consensus success probabilities of versus the number of nodes under different communication failure probability

Fig. 4.5 illustrates the consensus success probability of the cellular PBFT network under different coverage probabilities. When the communication success probability between the base stations and the PBFT nodes is high (i.e. 90% and 80%), the consensus success probability can reach the lower bound of the communication success probability 80%. Even when the communication success rate drops to 70%, the consensus success probability can still increase as the size of the network increases. However, when the communication success rate further drops to 60%, the consensus success probability stays at the minimum level and decreases as the number of PBFT nodes increases. This result indicates that the cellular PBFT network is scalable and tolerant to node loss when the inter-node communication achieves a good performance.

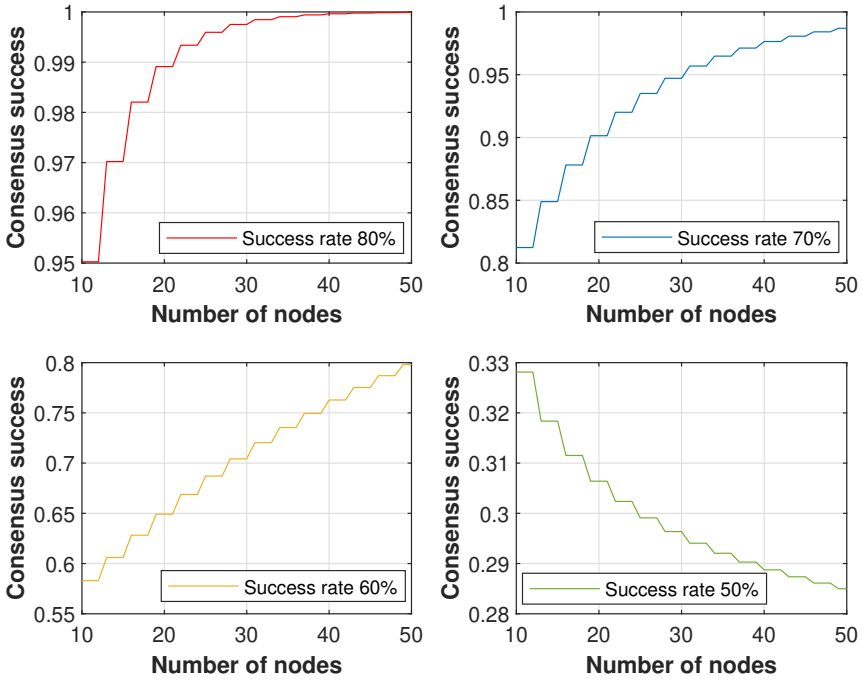

Figure 4.6: Consensus success probability of comparison with f deterministic byzantine nodes success rate

Fig. 4.6 demonstrates the consensus probability of the case where there are $f = \lfloor \frac{n-1}{3} \rfloor$ deterministic byzantine nodes in the network. The plots under different communication success rates follow a similar trend as in Fig. 4.5. When the communication success rate is high, the consensus success probability increases with the number of nodes. Once the success rate drops below a certain value, the consensus success probability declines. It is worth noting that the consensus success probability is higher even though the PBFT network has reached its maximum byzantine tolerance threshold. This shows that the byzantine fault is

more harmful when it is arbitrary. If their presence is known and determined, the system only needs fewer resources to tackle them.

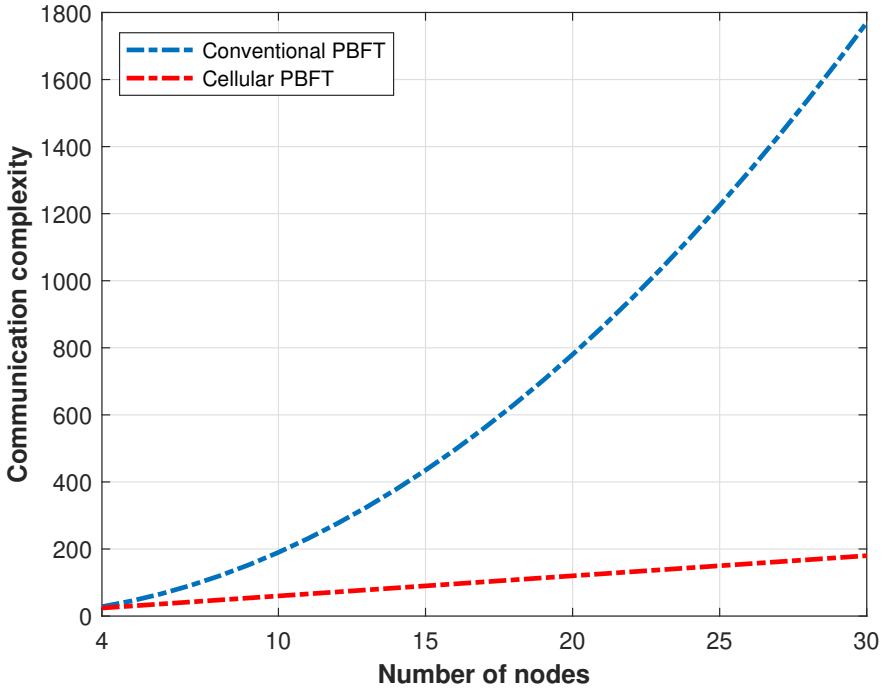

Figure 4.7: Communication complexity of traditional PBFT versus PBFT in the cellular network

Fig. 4.7 compares the communication complexities of the conventional PBFT, where the consensus is reached through direct inter-node communications, and PBFT implemented over the cellular network where the inter-node communication relies on the base station. As shown in Fig. 4.7, the communication complexity of PBFT follows an exponential increase while the cellular PBFT's communication complexity increases linearly. The cellular PBFT outperforms the conventional PBFT with much lower communication complexity after a similar communication complexity stage where $n \leq 5$.

Fig. 4.8 presents the view change occurrence probability and the average view change delay versus the different number of nodes in the PBFT network. The solid lines show the view change delay and view change occurrence probability, where $f = \lfloor \frac{n-1}{3} \rfloor$. The view change is more likely to happen as the network scales up, and the average view change delay increases as well. However, the increase of view change occurrence probability is subtle compared to the view change delay. This is due to the fact that the proportion of faulty nodes to the total nodes is the same. The phenomenon that view change delay increases more indicates that the number of faulty nodes has bigger weights on the average view change

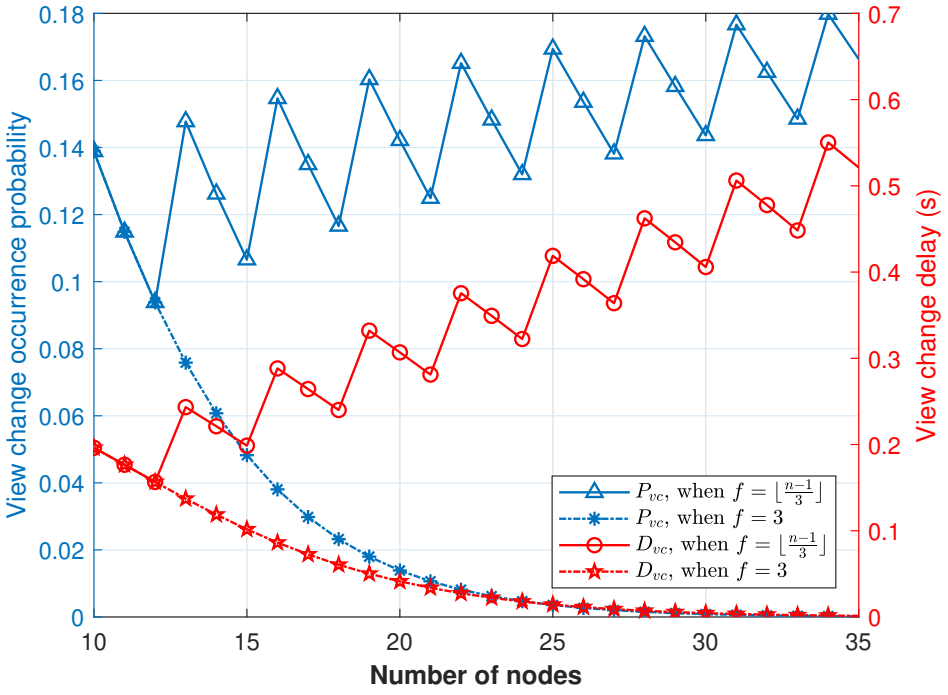

Figure 4.8: View change occurrence probability and delay in the cellular PBFT network

delay. The dotted lines show the view change delay and view change occurrence probability, where $f = 3$. It can be seen that the impacts of faulty nodes on the view change are minimised as the proportion of the faulty nodes decreases.

Fig. 4.9 demonstrates the consensus delay and throughput versus the utilization factor ρ. This study considers a packet length of $8,584$ bits and a transmission rate of 1 Mbps for the base stations. The cellular achieves a high consensus throughput and low delay. As derived in Section VI, the consensus throughput and delay are related to the base station's transmission rate and the amount of data. With more nodes in the PBFT network, the data amount correspondingly rises, and the bandwidth of the base station can be tuned to satisfy the needs of the network. Thus, scalability can be robust, provided the base station has sufficient bandwidth.

Fig. 4.10 illustrates both the energy consumption of a single node and the comparison between the overall energy consumption of the traditional PBFT network and the PBFT system in a cellular network. It highlights the sustainability of the network and demonstrates the improved energy efficiency of the cellular PBFT system.

Fig. 4.11 compares the average node transmit power required in the conventional

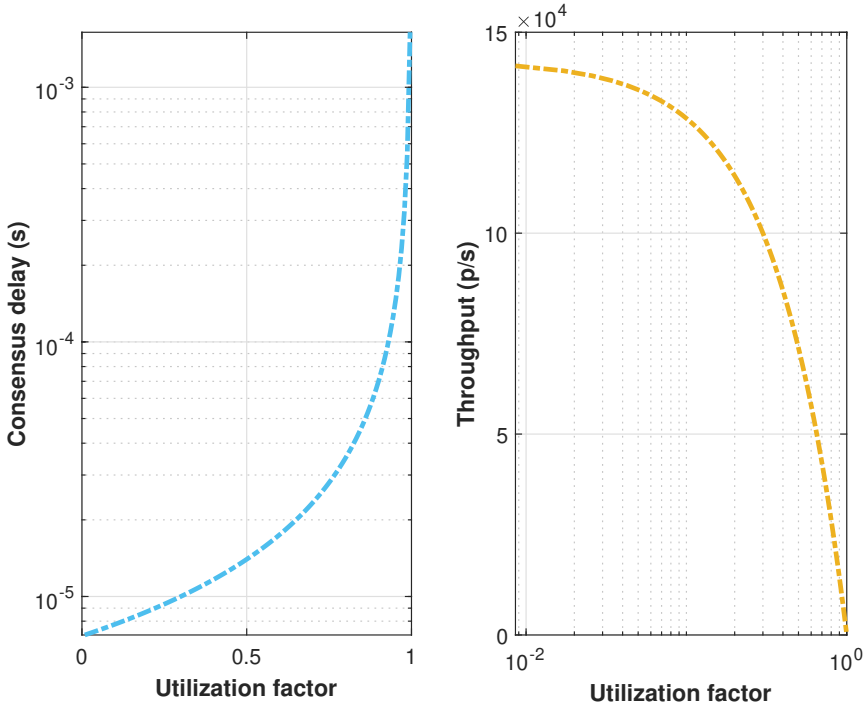

Figure 4.9: Consensus delay and throughput versus ρ in the cellular PBFT network

PBFT and BS-enabled PBFT networks. The conventional and BS-enabled PBFT simulation results are also provided for verification. The simulation results are obtained by averaging over 10000 trials. A tight match can be seen between the simulation and analytical results. It can be seen in Fig. 4.11 that the transmit power increases exponentially with the coverage radius. Moreover, the BS-enabled PBFT network consumes approximately 82.4% less transmission power. This makes the BS-enabled PBFT network more advantageous, as the PBFT nodes are usually power-constrained devices.

4.4.1 Optimal Configuration

As shown in Fig. 4.5 and Fig. 4.6, when the success rates are high (above 70%), the consensus success rate keeps increasing with the network size scaling up, and decreases when the success rate is 60%. When the success rate is even higher (above 80%), the consensus success rate approaches 1. This phenomenon indicates that there is a turning point in the success rate where the consensus starts to drop and an optimal point where the consensus rate can reach an ideal performance.

As shown in Section III.A, the consensus success probability follows a binomial distribution $X \sim (n, P)$, where n is the number of nodes and P is the coverage

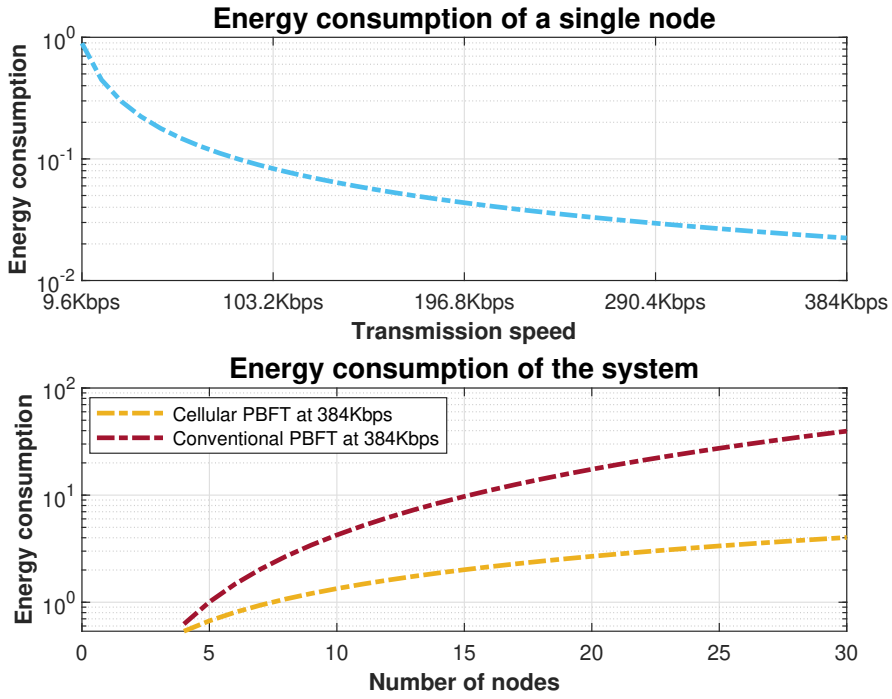

Figure 4.10: Energy consumption of a single node and the whole system

probability. According to De Moivre–Laplace theorem [121], given a sufficiently large number of n, a binomial distribution can be approximated to a normal distribution. The binomial distribution represents the number of successes in n independent experiments. The normal case operation of PBFT requires up to $2f + 1$ successes in each phase. Hence, the success probability only counts when more than $2f + 1$ nodes are involved, as shown in Fig. 4.12, where the red box is the countable window of the PBFT. The mean μ of the binomial distribution is determined by n and P, as $\mu = nP$. The middle line of the distribution sits on the mean value. Thus, for a fixed n, as the mean value decreases with the P, the overall distribution moves to the left, resulting in the overall success probability decreasing accordingly.

To find the optimal value of P for an ideal consensus success probability, a target consensus success probability should be set. For instance, the target consensus success probability is set to 80%. The distribution is approximated as a normal distribution with a pdf of $P(X = x)$, and the total value of the bars is assumed to sum to 1. To find the 80% to the right, it is approximated that the distribution is symmetric about the mean value at μ. Equivalently, we need to find the value of $z > 0$ such that $Pr(Z < -z) = 0.2$ under a standard normal distribution. According to the z-score table [122], $-z = -0.84$. Therefore, the consensus success probability is greater than 80% when $Z \geq -0.84$. For non-normal

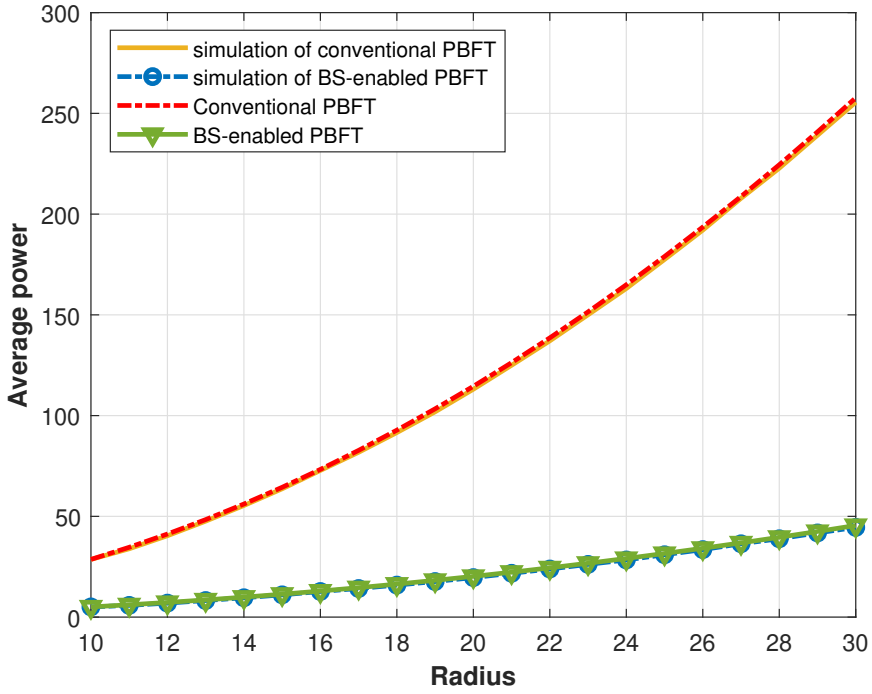

Figure 4.11: Average transmit power versus radius

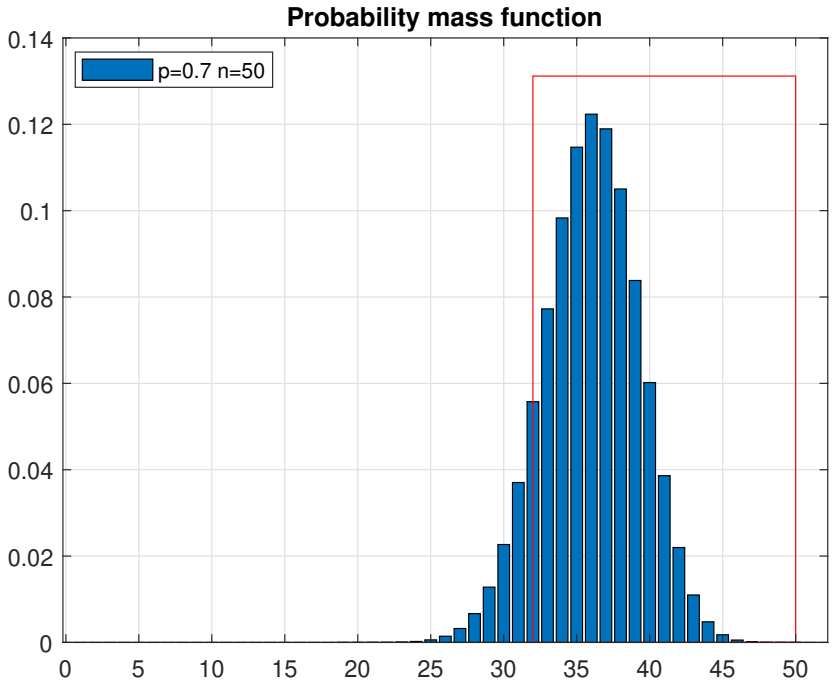

Figure 4.12: Binomial distribution and countable window

distribution, it can be standardized with mean μ and standard deviation σ as

$$Z = \frac{X - \mu}{\sigma}. \tag{4.54}$$

It becomes

$$\frac{X - \mu}{\sigma} \geq -0.84. \tag{4.55}$$

Then,

$$X \geq \mu - 0.84\sigma. \tag{4.56}$$

Correlating it to the requirement of PBFT, and given that $\mu = nP$ and $\sigma = \sqrt{nP(1-P)}$, it further transforms to

$$nP - 0.84\sqrt{nP(1-P)} \geq n - f. \tag{4.57}$$

Moreover, with the fact that $f = \left\lfloor \frac{n-1}{3} \right\rfloor$, the correlation between the optimal P and number of nodes n can be approximated as

$$P \geq \frac{\frac{4}{3}n + 1.372 + \frac{1}{3}\sqrt{5.645n + 1.658 - \frac{2.822}{n}}}{2n + 1.411}, \tag{4.58}$$

where the minimum optimal P can be obtained by applying different n, while guaranteeing the consensus success probability is greater 80%.

For other desired consensus success probability, if the corresponding value on the z-score table is $\mathcal{A}$, the relationship between the optimal P and number of nodes n is then given by

$$P \geq \frac{\frac{4n+2}{3} + \mathcal{A}^2 + \frac{1}{3}\sqrt{8\mathcal{A}^2 n + 9\mathcal{A}^4 - 4\mathcal{A}^2 - \frac{4}{n}\mathcal{A}^2}}{2n + 1.411}, \tag{4.59}$$

As P is relevant to the SINR, Poison distribution intensity λ, and path loss exponent α. Hence, guided by the optimal P, under a specific λ and α, an appropriate SINR threshold can be tuned for better performance. For example, in Fig. 4.13, the minimum coverage probability for achieving 80% consensus success probability is about 0.75 when $n = 26$. According to Fig. 4.4, the SINR threshold should be set to approximately -5 dB for the downlink communication and approximately -8 dB for the uplink communication.

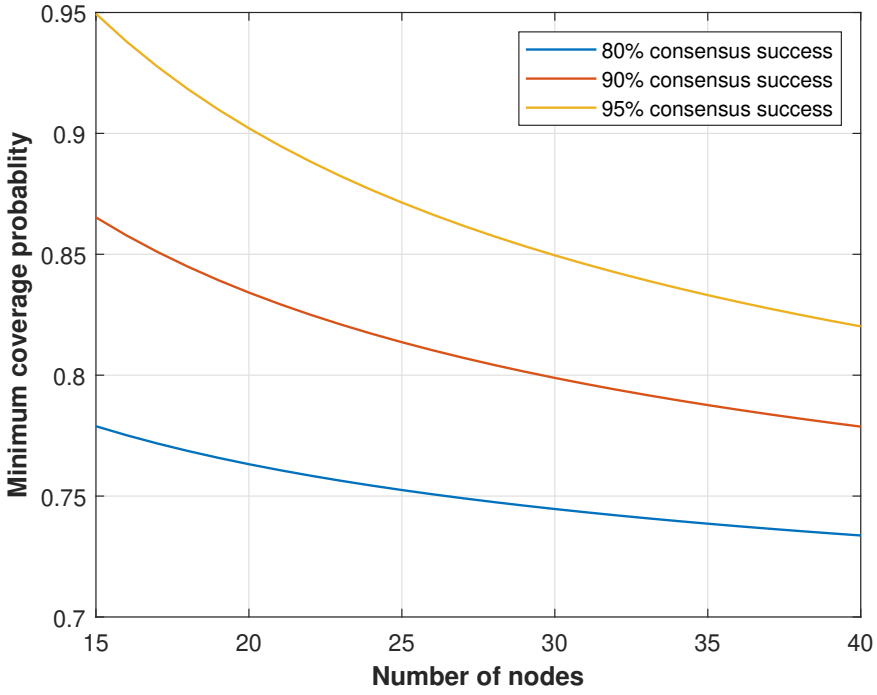

Figure 4.13: Minimum coverage probability for achieving 80% consensus success probability

4.5 Security Risk

Even though the base station enables inter-node communications, PBFT can achieve better consensus success probability, lower communication complexity, delay, and higher throughput, there are some security risks associated with the base station. They can be summarised as follows:

- **Centralisation:** The goal of blockchain is to establish consensus in a distributed and decentralized way within an untrusted environment. However, relying on base stations for inter-node communication introduces a degree of centralisation to the blockchain system.
- **Lower security:** The inter-node communications rely on the base stations, potentially lowering the system's security, especially if the base stations are compromised or subjected to malicious attacks. In such cases, the nodes' messages may be dropped or tampered with by the base station, which further influences the validity of the consensus.
- **Privacy leakage:** In the downlink communication of the cellular PBFT network, the base stations broadcast the aggregated messages to the nodes. However, such messages may be captured by other users within the coverage

of the base station, which leads to the privacy leakage of the consensus.

- **Mobility issue:** In the cellular PBFT network, the node can be mobile, necessitating handover between adjacent cells. This can lead to increased power of the nodes. Moreover, if a node moves to a cell serviced by a different network operator, roaming is therefore required, which may cause delays and interruptions.

The issues mentioned above may hinder the deployment of the PBFT over cellular networks, but they can be mitigated by embracing some techniques. For example, encryption and cryptography can be incorporated to mitigate security and privacy issues [123], and predictive handover facilitated by machine learning can address the mobility issue [124].

4.6 Conclusion

This chapter presents a novel scheme for the PBFT network, where the internode communications of the normal case operation are done through the base stations. The scheme is discussed with two scenarios: a single-base-station-enabled, and multiple-base-stations-enabled PBFT network. The performance of the proposed scheme is evaluated through the consensus success probability, average transmit power, view change delay and occurrence probability, consensus delay and throughput. A special case where a network's consensus success probability with f deterministic byzantine nodes is investigated. The numerical results show that, compared to the conventional PBFT network, the cellular PBFT network achieves higher consensus success probability, higher scalability, less power consumption, less communication complexity, and low consensus delay. In addition, an optimal configuration of the P and the SINR under different network sizes is discussed. However, as the internode communication entirely depends on the base stations, the compromise of base stations would paralyze the PBFT network.

Chapter 5

The Security of a Hybrid PBFT Consensus Network

This chapter investigates the view change delay and occurrence probability in the base station-enabled PBFT network. Even though view change provides liveness and resilience to the system, frequent view changes due to network failure and collisions could undermine the overall performance by delaying the generation of consensus. Moreover, the wireless network suffers not only from collisions and crashes but also from malicious attacks. In this regard, this chapter discusses the security of a hybrid PBFT consensus network in the presence of malicious attacks and crashes, where a private and a public cloud comprise the network. The security level is analysed under various network parameters across two distinct coordination modes. A special case involving a secure private cloud is further examined.

5.1 Introduction

The performance of the wireless channel significantly impacts the security and efficiency of the PBFT network, as discussed in [125]. This is especially true in the ad hoc network where nodes contend for medium access. As the network size increases, collisions become more frequent, impairing the scalability of the wireless PBFT network. Another issue introduced by wireless networks is the view change mechanism. View change ensures the liveness of PBFT by replacing the primary nodes if it fails, preventing the system from waiting indefinitely [73]. However, frequent view changes can undermine network efficiency by delaying consensus. In a wireless environment, primary nodes are more likely to be faulty due to network instability. To address these challenges, a hybrid PBFT network is proposed in [126], wherein the PBFT network is divided into private and public clouds. In the private cloud, all nodes are reliable but may still compromise due to crashes, while in the public cloud, nodes may be prone to crashes or malicious behaviours. If the primary node resides in the private cloud, concerns related to view change are mitigated, and the security of the PBFT network can be enhanced by increasing the proportion of private nodes.

Blockchain records all transactions on a distributed ledger shared by all nodes, providing traceability [127] for failures and malfunctions in the event of network compromises. This enhances the problem-solving capability of the wireless network. Permissioned blockchain is operated by a group of trusted entities. Unlike public blockchains like Bitcoin, in which anyone can participate and get access to the chain, permissioned or private blockchain [128] runs with controlled access such that only authorised participants can join the network. Hence, the permission blockchain can be deployed for anomaly detection [129] and identity management [36] in the wireless network. Moreover, a key enabler of blockchain technology is the smart contract, which enforces predefined rules and terms if the conditions are met. In this regard, blockchain can be deployed in the wireless network for network orchestration and automation [130]. Another critical aspect of blockchain is its incentivization mechanism [131], which motivates individuals to participate, ensuring the integrity and robustness of the network. In Bitcoin, miners are incentivized according to the computing power they contribute while pursuing hash values. Similarly, blockchain can be leveraged for spectrum sharing in wireless networks [132], where nodes that share spectrum are incentivized accordingly. Implementing blockchain technology in wireless networks enhances node availability and network connectivity. The hybrid PBFT network not only provides Byzantine fault tolerance but also enables applications in wireless

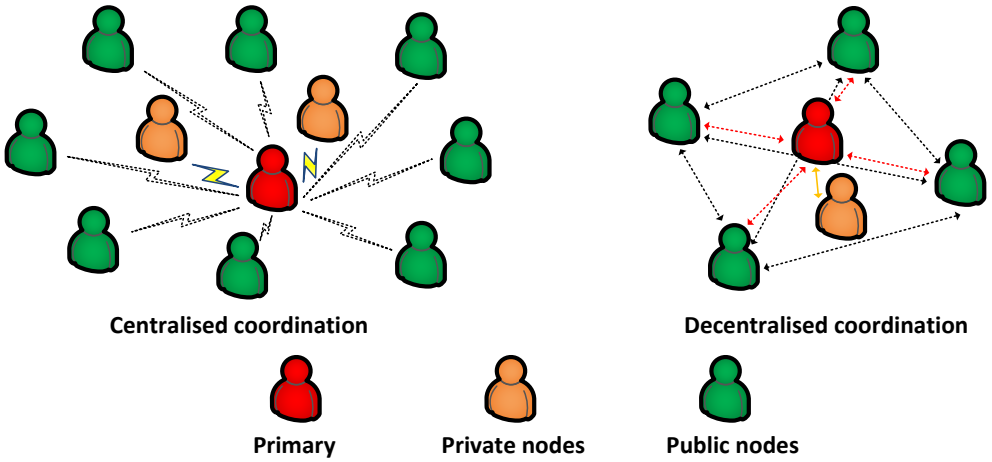

Figure 5.1: PBFT under centralised coordination versus decentralised coordination

networks where nodes are prone to crashes, failures, and potential malicious attacks, thereby enhancing network and applications' reliability.

5.2 System Model

The PBFT network consists of two types of nodes: a primary node and backup nodes. Consensus is achieved through the normal case operation, as illustrated in Fig. 2.1. The primary node collects a request from the client and initiates a consensus process by sending a *pre-prepare* message to the backups. A valid consensus is reached only after the inter-node communications in the prepare and commit phases meet the required conditions. In the original PBFT protocol, the primary node could be faulty, necessitating the view change mechanism to select a new primary to ensure the network's liveness.

In the hybrid PBFT model, the network is composed of nodes from the private and public cloud. Nodes in the private cloud are verified and assumed to be trusted and non-malicious, endorsed by the reputation system, though they can still crash due to link failures or collisions. The primary node is selected from these private nodes to reduce the probability of view changes and enhance the overall network efficiency. Therefore, the view change mechanism is primarily triggered by the view change timeout in this model. Nodes in the public cloud are untrusted and may experience crashes or be subjected to malicious attacks. Crashes in the public cloud can cause nodes to become non-responsive or prevent them from sending messages due to link failures or collisions. Malicious attacks refer to nodes behaving adversarially to subvert consensus by sending deceptive or disruptive messages.

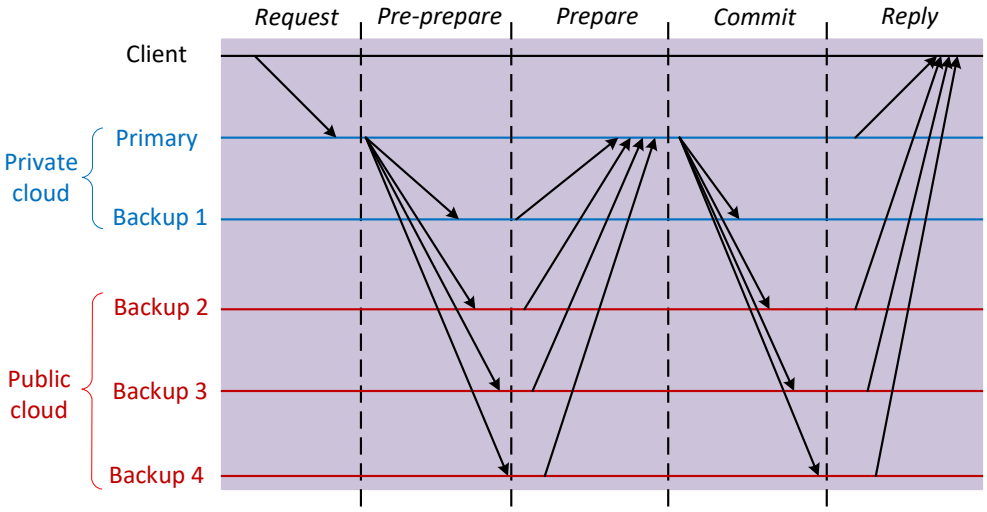

Figure 5.2: Centralised coordination

Suppose there are n_c nodes in the private cloud and n_p in the public, and the network can tolerate up to f faulty nodes. The relationship between n_c, n_p and f is given by

$$f \leq \left\lfloor \frac{n_c + n_p - 1}{3} \right\rfloor. \tag{5.1}$$

According to [73], the PBFT network can tolerate up to f faulty nodes, which can be either malicious or not responding. In the worst scenario, all f malicious nodes are involved in the normal case operation. To ensure the correctness of the consensus, at least $f + 1$ non-faulty nodes must participate in the normal case operation. Therefore, the validity of the consensus is only confirmed when the client receives at least $f + 1$ matching replies.

The Hybrid PBFT network can be set up in two modes: centralised coordination and decentralised coordination, as shown in Fig. 5.1. The two modes of the normal case operation of the hybrid PBFT network are illustrated in Fig 5.2 and 5.3.

In the centralised coordination mode as dicpited in Fig. 5.2, backup nodes do not communicate directly with each other; instead, they communicate through the primary node, which acts as a coordinator between nodes in the private and public clouds. The normal case operation proceeds as follows:

Pre-prepare: After receiving a request from the client, the primary broadcasts a *pre-prepare* message to all backup nodes.

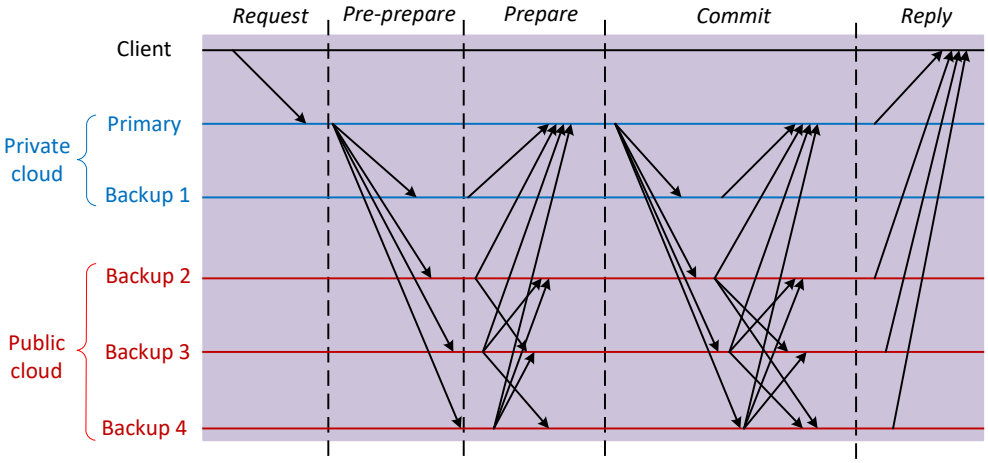

Figure 5.3: Decentralised coordination

Prepare: Upon receiving the *pre-prepare* message, a backup node enters the prepare phase and sends a *prepare* message back to the primary node.

Commit: The primary node broadcasts *commit* messages to all backup nodes only if it receives enough valid *prepare* messages.

Reply: All public backup nodes and the primary send a *reply* message to the client.

To save communication resources, only the primary sends the *reply* message on behalf of the private cloud, as private nodes are fully trusted.

In the decentralised mode as depicted in Fig. 5.3, the workflow within the private cloud remains unchanged, but the public nodes exchange information directly with each other. During the normal case operation, the process is as follows:

Pre-prepare: After receiving a request from the client, the primary node broadcasts a *pre-prepare* message to all backup nodes.

Prepare: Upon receiving a valid *pre-prepare* message,

- private backup nodes send a *prepare* message directly to the primary node.
- public backup nodes broadcast a *prepare* message to both other public backup nodes and the primary node.

Commit:

- Upon receiving enough valid *prepare* messages from the public cloud, the primary node broadcasts a *commit* message to the public cloud,

including the *prepare* messages from the private cloud.

- Upon receiving enough valid *prepare* messages plus the *commit* message from the primary, public backup nodes broadcast a *commit* message to other public backup nodes and the primary node.

Reply: All public backups and the primary node send a *reply* message to the client.

It is worth noting that the cross-cloud communication between backups is not possible.

5.3 Security of the Hybrid PBFT Networks

The security of PBFT networks is assessed by the consensus success probability. In our model, we assume that communications in the private and public cloud are subject to crashes. In the decentralised coordination mode, crashes result from collisions, while in the centralised coordination mode, crashes are due to hidden nodes. Although these two scenarios may have different probabilities, for simplicity, we use a general probability P_c to denote the crash probability of private and public cloud communications. Additionally, the malicious rate in the public cloud is denoted by P_m.

A valid consensus must successfully navigate the entire normal case operation process. Therefore, the consensus success probability for both modes is derived phase by phase.

5.3.1 Decentralised Coordination

Pre-prepare Phase Success Probability

In this phase, the primary node is fully trusted and is assumed to achieve a 100% success probability in transmitting the *pre-prepare* message. This assumption also holds when only the primary uses the channel, with no channel contention occurring, as seen in the commit phase of both modes shown in Fig. 5.2 and Fig. 5.3.

Prepare Phase Success Probability

Given the 100% success rate in the pre-prepare phase, all backup nodes should receive a *pre-prepare* message from the primary. To enter the commit phase, a node should receive at $2f$ *prepare* messages from the other nodes, with no more

than f of these messages coming from malicious nodes to ensure safety. Let N_p denote the number of *prepare* messages received by a node, and N_m denote the number of *prepare* messages from malicious nodes. The prepare phase success probability in the decentralised coordination mode can be defined by the CCDF as

$$P_{prepare} = \mathbb{P}(N_p >= 2f, N_m <= f) = \mathbb{P}(N_p >= 2f) \cdot \mathbb{P}(N_m <= f). \tag{5.2}$$

Let i denote the failed nodes due to crashes in the private cloud, m and F denote the failed nodes due to crashes and malicious nodes in the public cloud, respectively. Then, $\mathbb{P}(N_p >= 2f)$ can be expressed as in (5.3).

$$\mathbb{P}(N_p >= 2f) = \begin{cases} \sum_{i=0}^{f} \binom{n_c-1}{i} (1-P_c)^{n_c-1-i} {P_c}^i \sum_{m=n_p+i-f}^{n_p} \binom{n_c-1}{m} \\ \qquad (1-P_c)^m {P_c}^{n_p+i-m}, & n_c - 1 \geq f \\ \sum_{i=0}^{n_c-1} \binom{n_c-1}{i} (1-P_c)^{n_c-1-i} {P_c}^i \sum_{m=n_p+i-f}^{n_p} \binom{n_c-1}{m} \\ \qquad (1-P_c)^m {P_c}^{n_p+i-m}, & n_c - 1 < f \end{cases} \tag{5.3}$$

Furthermore,

$$\mathbb{P}(N_m <= f) = \begin{cases} \sum_{F=0}^{f} \binom{m}{F} {P_m}^F (1-P_m)^{m-F}, & m \geq f \\ \sum_{F=0}^{m} \binom{m}{F} {P_m}^F (1-P_m)^{m-F}, & m < f. \end{cases} \tag{5.4}$$

Combining (5.3) and (5.4), the prepare phase success probability $P_{prepare}$ is given by P in (5.5).

$$P = \begin{cases} \dfrac{\sum_{i=0}^{f} \binom{n_c-1}{i} (1-P_c)^{n_c-1-i} {P_c}^i \sum_{m=n_p+i-f}^{n_p} \binom{n_p}{m} (1-P_c)^m {P_c}^{n_p-m}}{\left(\sum_{F=0}^{f} \binom{m}{F} {P_m}^F (1-P_m)^{m-F}\right)}, & n_c - 1 \geq f, m \geq f \\ \dfrac{\sum_{i=0}^{n_c-1} \binom{n_c-1}{i} (1-P_c)^{n_c-1-i} {P_c}^i \sum_{m=n_p+i-f}^{n_p} \binom{n_p}{m} (1-P_c)^m {P_c}^{n_p-m}}{\left(\sum_{F=0}^{f} \binom{m}{F} {P_m}^F (1-P_m)^{m-F}\right)}, & n_c - 1 < f, m \geq f \\ \dfrac{\sum_{i=0}^{f} \binom{n_c-1}{i} (1-P_c)^{n_c-1-i} {P_c}^i \sum_{m=n_p+i-f}^{n_p} \binom{n_p}{m} (1-P_c)^m {P_c}^{n_p-m}}{\left(\sum_{F=0}^{m} \binom{m}{F} {P_m}^F (1-P_m)^{m-F}\right)}, & n_c - 1 \geq f, m < f \\ \dfrac{\sum_{i=0}^{n_c-1} \binom{n_c-1}{i} (1-P_c)^{n_c-1-i} {P_c}^i \sum_{m=n_p+i-f}^{n_p} \binom{n_p}{m} (1-P_c)^m {P_c}^{n_p-m}}{\left(\sum_{F=0}^{m} \binom{m}{F} {P_m}^F (1-P_m)^{m-F}\right)}, & n_c - 1 < f, m < f \end{cases} \tag{5.5}$$

Commit Phase Success Probability

The flow of the commit phase closely mirrors that of the prepare phase. Firstly, the primary broadcasts a *commit* message containing the *prepare* messages from the private cloud to the public nodes. Then, the public nodes proceed with the commit phase by sending a *commit* message to other public nodes and the primary node. As each public node has received the *commit* message from the primary, the validity of the *commit* is confirmed when a node receives at least $2f$ *commit* messages, with no more than f of these coming from malicious nodes. Let N_c denote the number of messages received by a node. The success probability of the commit phase in the decentralised coordination mode can be defined by the CCDF as follows

$$P_{commit} = \mathbb{P}(N_c >= 2f, N_m <= f) = \mathbb{P}(N_c >= 2f) \cdot \mathbb{P}(N_m <= f), \tag{5.6}$$

which is equivalent to the probability P in (5.5) for the prepare phase.

Therefore, we have

$$P_{commit} = P_{prepare} = P. \tag{5.7}$$

End-to-end Consensus Success Probability

A consensus is confirmed when the whole normal case operation is completed.

Theorem 9. *The end-to-end consensus success probability P_{con} under decentralised coordination mode is given in (5.8).*

$$P_{con} = \begin{cases} \left(\sum_{i=0}^{f}\sum_{m=n_p+i-f}^{n_p}\binom{n_c-1}{i}\binom{n_p}{m}(1-P_c)^{n_c-1-i+m}{P_c}^{n_p+i-m} \left(\sum_{F=0}^{f}\binom{m}{F}{P_m}^{F}(1-P_m)^{m-F}\right)\right)^2, & n_c-1\geq f, m\geq f \\ \left(\sum_{i=0}^{n_c-1}\sum_{m=n_p+i-f}^{n_p}\binom{n_c-1}{i}\binom{n_p}{m}(1-P_c)^{n_c-1-i+m}{P_c}^{n_p+i-m} \left(\sum_{F=0}^{f}\binom{m}{F}{P_m}^{F}(1-P_m)^{m-F}\right)\right)^2, & n_c-1< f, m\geq f \\ \left(\sum_{i=0}^{f}\sum_{m=n_p+i-f}^{n_p}\binom{n_c-1}{i}\binom{n_p}{m}(1-P_c)^{n_c-1-i+m}{P_c}^{n_p+i-m} \left(\sum_{F=0}^{m}\binom{m}{F}{P_m}^{F}(1-P_m)^{m-F}\right)\right)^2, & n_c-1\geq f, m< f \\ \left(\sum_{i=0}^{n_c-1}\sum_{m=n_p+i-f}^{n_p}\binom{n_c-1}{i}\binom{n_p}{m}(1-P_c)^{n_c-1-i+m}{P_c}^{n_p+i-m} \left(\sum_{F=0}^{m}\binom{m}{F}{P_m}^{F}(1-P_m)^{m-F}\right)\right)^2, & n_c-1< f, m< f \end{cases} \tag{5.8}$$

The above discussion only considers the inter-node communication within the private cloud, which relies on wireless communication. However, if the nodes in the private cloud are in a secure connection, ensuring no crashes occur within the private cloud, the security level of the hybrid PBFT network is further enhanced.

$$\overline{P}_{consensus} = \begin{cases} \left(\sum_{m=n_p-f}^{n_p}\binom{n_p}{m}(1-P_c)^{m}{P_c}^{n_p-m}\left(\sum_{F=0}^{f}\binom{m}{F}{P_m}^{F}(1-P_m)^{m-F}\right)\right)^2, & m\geq f \\ \left(\sum_{m=n_p-f}^{n_p}\binom{n_p}{m}(1-P_c)^{m}{P_c}^{n_p-m}\left(\sum_{F=0}^{m}\binom{m}{F}{P_m}^{F}(1-P_m)^{m-F}\right)\right)^2, & m< f \end{cases} \tag{5.9}$$

Corollary 9.1. *The end-to-end consensus success probability $\overline{P}_{consensus}$ in the decentralised mode with a secure private cloud is given in (5.9).*

5.3.2 Centralised Coordination

Pre-prepare Phase Success Probability

Similar to the centralised coordination mode, the primary can achieves 100% success probability in transmitting the *pre-prepare* message.

Prepare Phase Success Probability

Given that all public nodes have received the *pre-prepare* message, they return the *prepare* message to the primary via unicast. In this case, the channel contention results from the hidden nodes. The prepare phase success probability under centralised coordination mode can be defined using the CCDF as

$$\overline{P}_{prepare} = \mathbb{P}(N_p >= 2f, N_m <= f) = \mathbb{P}(N_p >= 2f) \cdot \mathbb{P}(N_m <= f), \qquad (5.10)$$

where (5.5) provides the same expression.

Commit Phase Success Probability

The success of the commit phase is contingent upon the primary node receiving at least $2f$ *prepare* messages. In this phase, the primary broadcasts this information to the public nodes. Given that only the primary node transmits during this phase, the commit phase success probability in the centralised coordination mode is assumed to be 100%.

End-to-end Consensus Success Probability

Based on the above discussion, the end-to-end consensus success probability depends solely on the prepare phase.

Theorem 10. *The end-to-end consensus success probability in the centralised mode is equivalent to P in (5.5), since the pre-prapare and commit phases achieve 100*

It is worth noting that the centralised coordination mode significantly reduces the communication complexity, conserves massive communication resources and demonstrates that consensus can be achieved within just one effective phase if the primary is trusted.

Corollary 10.1. *The end-to-end consensus success probability $\overline{P}$ in the centralised modes with a secure private cloud is given in (5.11).*

$$\overline{P} = \begin{cases} \sum_{m=n_p-f}^{n_p} \binom{n_p}{m}(1-P_c)^m {P_c}^{n_p-m}\left(\sum_{F=0}^{f}\binom{m}{F}{P_m}^F(1-P_m)^{m-F}\right), & m > f \\ \sum_{m=n_p-f}^{n_p} \binom{n_p}{m}(1-P_c)^m {P_c}^{n_p-m}\left(\sum_{F=0}^{m}\binom{m}{F}{P_m}^F(1-P_m)^{m-F}\right), & m \leq f \end{cases} \qquad (5.11)$$

5.4 Numerical Results and Discussion

This section presents the numerical results to showcase the security of the hybrid PBFT network for both centralised and decentralised modes and the effects of different parameters on its security. The frequently appeared notations are summarised in Table 5.1.

P_c	Probability of crash
P_m	Probability of malicious attacks
n_c	Number of private nodes
n_p	Number of public nodes

Table 5.1: Frequent notations

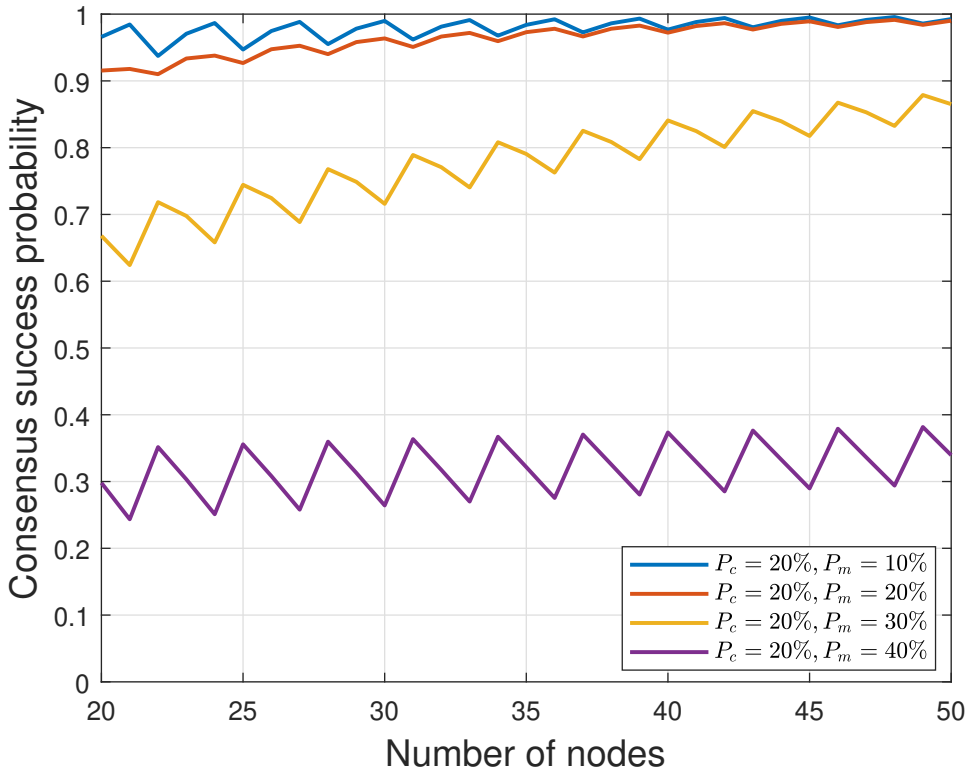

Figure 5.4: Benckmark consensus success probability versus the number of nodes with fixed P_c and varied P_m

Fig. 5.4 illustrates the benchmark security performance of the PBFT network in the presence of crashes and malicious attacks, showing the security level with fixed P_c and varied P_m. As can be seen in the plot, given the crash rate is 20%, the network can achieve an excellent performance even when the percentage of the malicious nodes is 10% and 20%. This indicates the robustness and resilience of the hybrid network against malicious attacks and crashes.

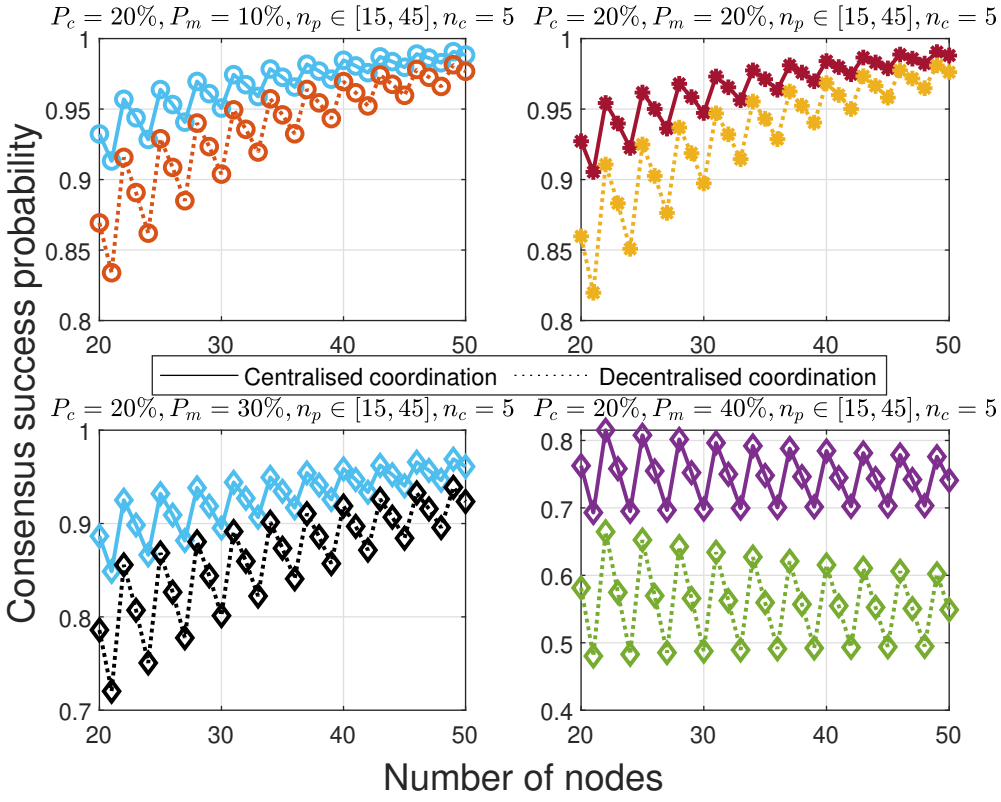

Figure 5.5: Consensus success probability with insecure private cloud versus the number of nodes with fixed P_c and varied P_m

Fig. 5.5 compares the security level of the hybrid PBFT network with an insecure private cloud under a fixed P_c, a constant number of private nodes n_c and varying P_m. The hybrid network can achieve a good security level when P_c and P_m are at a relatively low level. As the number of PBFT nodes increases, the security level increases accordingly, consistent with the trend observed in Fig 5.4. However, when P_m exceeds a certain threshold (around 40%), the security level declines as the network scales up.

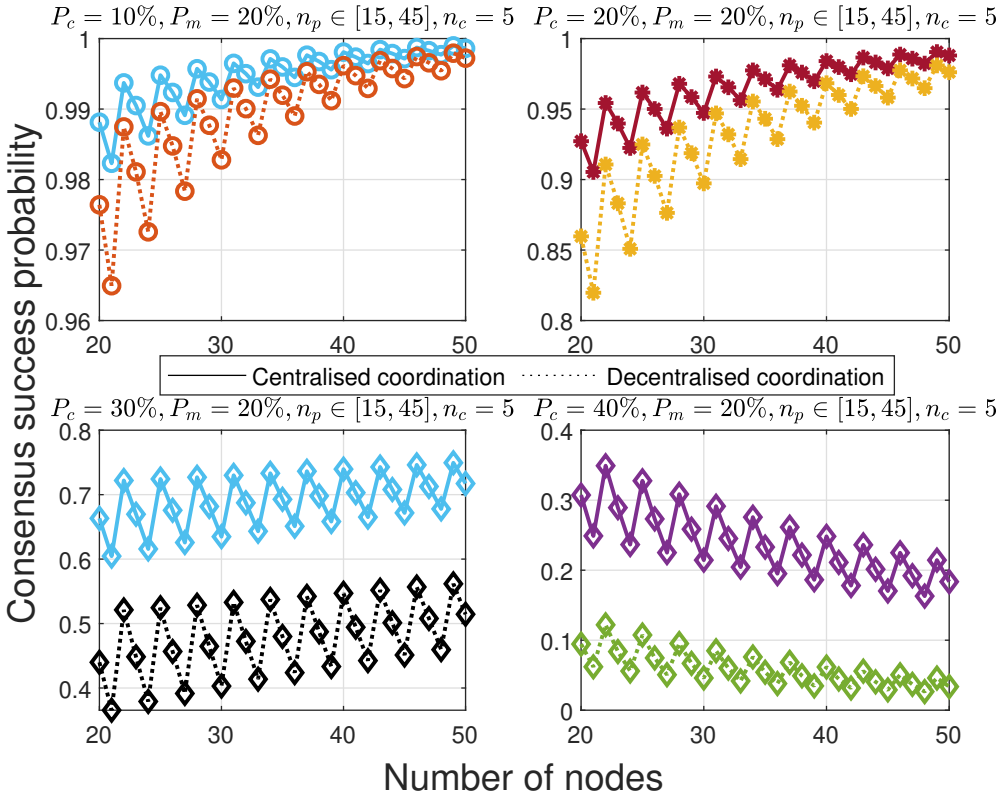

Figure 5.6: Consensus success probability with insecure private cloud versus the number of nodes with varied P_c and fixed P_m

Fig. 5.6 compares the security level of the hybrid PBFT network with an insecure private cloud under a fixed P_m, n_c and varied P_c. The overall trend is similar to Fig. 5.5. However, as P_c increases, the security decreases more rapidly, particularly in the third and fourth subplots. This indicates that the hybrid PBFT network is more sensitive to crashes than to malicious attacks highlighting the critical importance of wireless channel quality in determining the security of the PBFT network.

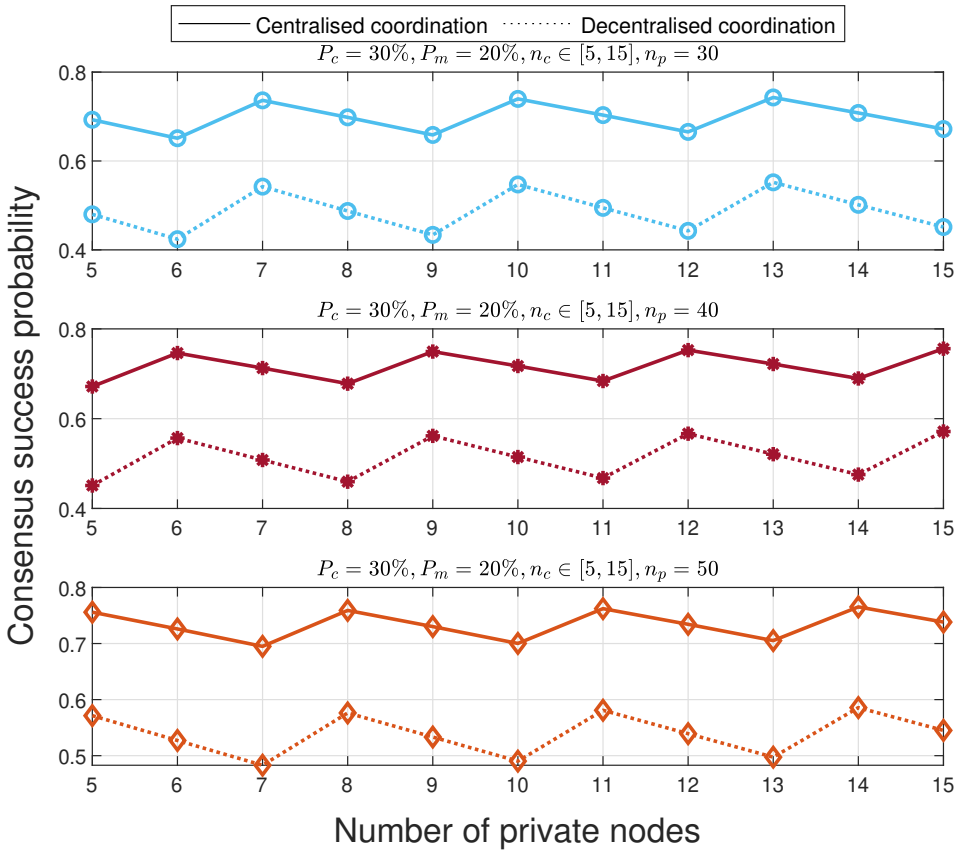

Figure 5.7: Consensus success probability with insecure private cloud versus the number of nodes with P_c and varied P_m

Fig. 5.7 illustrates the security level of the hybrid PBFT network when the private nodes increase from 5 to 15. The security level fluctuates around a certain level, as the crashes also happen in the private cloud. Increasing the number of private nodes does not enhance the security of the network.

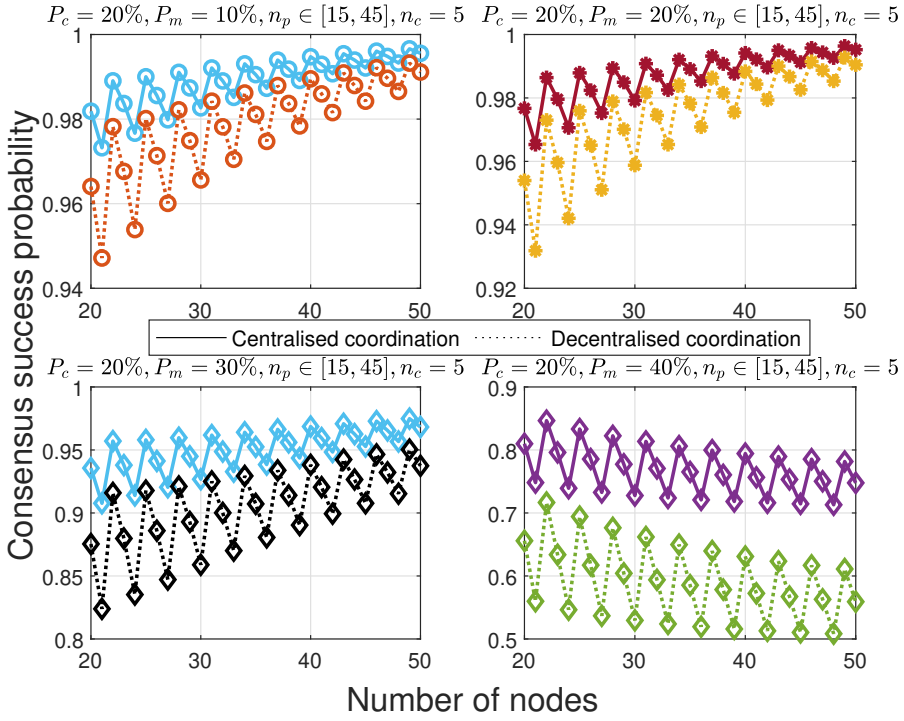

Figure 5.8: Consensus success probability versus the number of nodes with fixed P_c and varied P_m

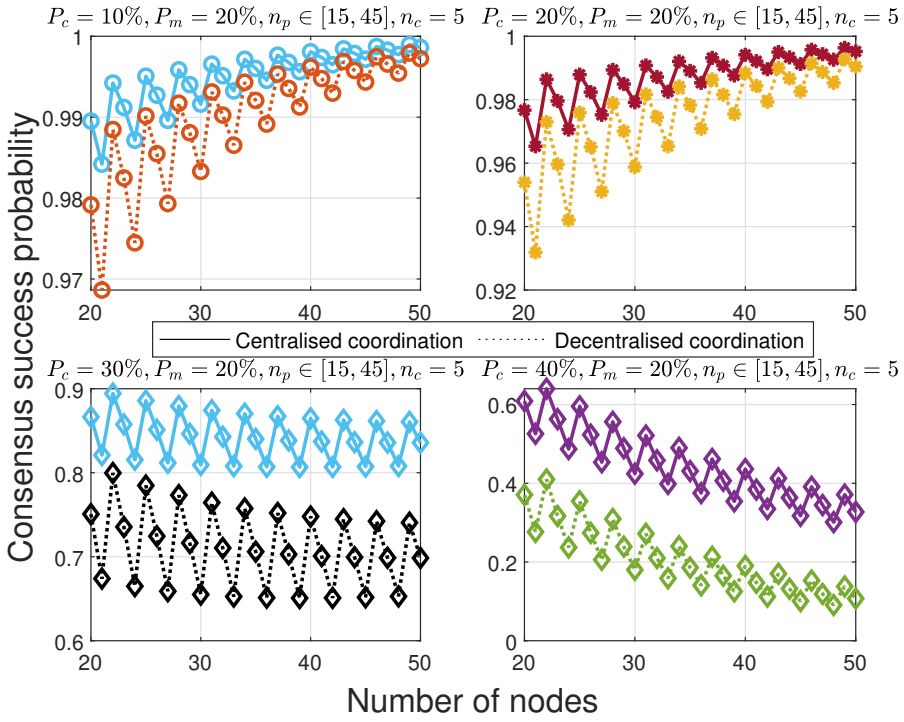

Figure 5.9: Consensus success probability versus the number of nodes with fixed P_m and varied P_c

Fig. 5.8 and Fig. 5.9 present the security level of the hybrid PBFT network with a secure private cloud, varying P_m and P_c, respectively. The trends are consistent with those in the case of insecure private cloud. However, a secure private cloud provides a higher security level, especially when P_c or P_m are high. Specifically, in the fourth subplot of Fig. 5.9, the consensus success probability is approximately 0.3 higher, compared to the insecure cloud scenario of Fig. 5.6 when the number of nodes is 20. This indicates that designing the PBFT network with a proportion of the nodes in a secure and stable environment significantly enhances consensus success.

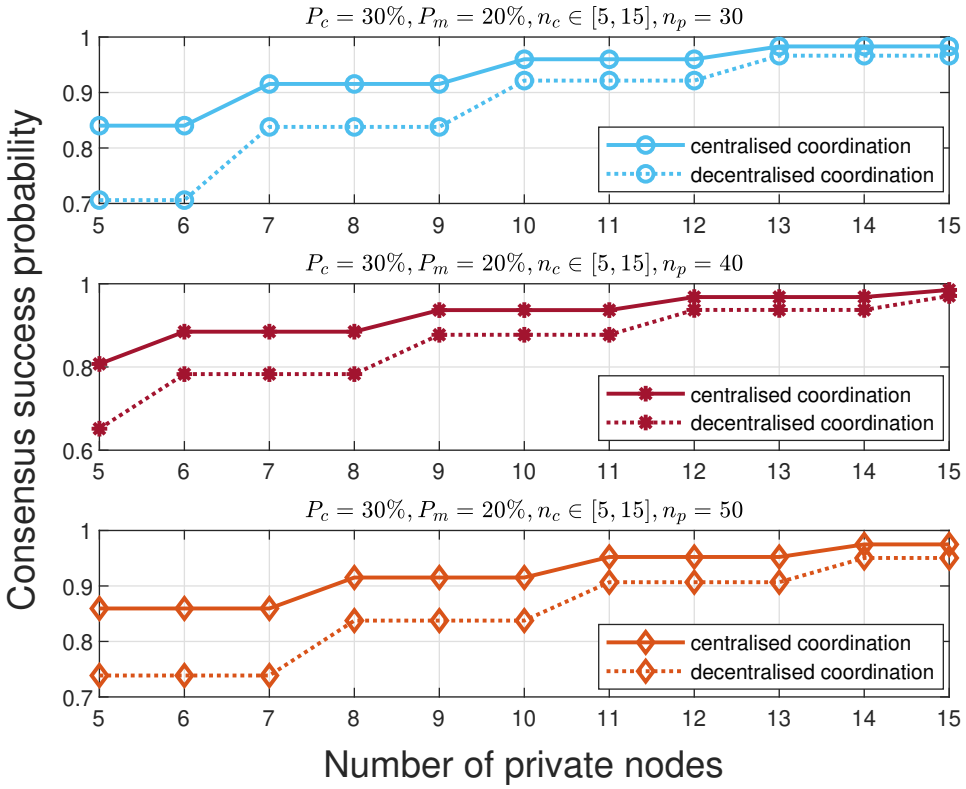

Figure 5.10: Consensus success probability versus number of nodes with varied n_p

Fig. 5.10 demonstrates the security performance of the hybrid network with varied n_p when n_c increases from 5 to 15. In contrast to Fig. 5.7, the security improves as the proportion of private nodes increases in the hybrid PBFT network. This further substantiates the benefits of incorporating a secure private cloud.

5.5 Conclusion

This chapter investigates the security level of the hybrid PBFT network in both centralised and decentralised modes, including a special case where the private cloud is secure and immune to crashes. The security level is demonstrated through the numerical results with various network parameters. The benchmark comparison indicates that incorporating the private cloud can significantly improve the security level of the PBFT network and eliminate the need for view changes. A secure private cloud can further enhance the security of the hybrid PBFT network. However, establishing a trusted and secure private cloud may require additional steps or techniques.

Chapter 6

Conclusion and Future Works

This thesis investigates and explores the feasibility of deploying the PBFT consensus mechanism with a practical wireless network or protocol. Specifically, the IEEE 802.11 broadcast scheme and cellular network are incorporated to implement the PBFT network. Moreover, a hybrid PBFT network is presented, and its security performance is investigated in the presence of crashes and malicious attacks. All models are underpinned by the analytical derivation and verified by the numerical results, which provide explicit guidance and optimization for future applications and deployment. The consensus success probability, consensus throughput, consensus delay, power consumption, view change delay, and communication complexity are the key performance indicators of wireless PBFT networks.

Chapter 1 provides the background of the current wireless network, which features the anticipation and limitations of the wireless network operated under the centralised scheme. The literature reviews and motivations of my research are also presented in this chapter.

Chapter 2 introduces wireless blockchain networks. Specifically, it presents the blockchain's fundamentals, including a comprehensive introduction to the consensus mechanism and its categories. Moreover, this chapter discusses the working procedures of the wireless blockchain network and some key performance indicators and attributes.

Chapter 3 proposes a framework for implementing the PBFT over a wireless channel using the IEEE 802.11 protocol. In this framework, nodes contend over the wireless channel. The transmission probability is, therefore, modelled using a Markov chain. The success probabilities for each phase, the end-to-end success

probability, transaction confirmation delay, and throughput are derived based on the transmission probability. The PBFT system provides liveness with the view change process. Hence, the view change delay in a wireless PBFT network using IEEE 802.11 protocol is analysed. We further investigate the impacts of the non-PBFT contention, which impairs the transmission mission success probability and increases the view change delay. The transmission success rate is determined by three parameters: network size (i.e., the number of nodes), contention window size, and packet arrival rate. Therefore, optimal pairs of packet arrival rate and contention window size under different network sizes are formulated to maximize the consensus's success probability without sacrificing the overall network performance.

Chapter 4 focuses on improving the scalability and connectivity of the wireless PBFT network by introducing a base station-enabled wireless PBFT network, where the inter-node communication of PBFT nodes goes through the base stations. To tackle the high communication complexity, a *timeout* mechanism is created. The performance of the base station-enabled wireless PBFT network is evaluated through the consensus success probability, average transmit power, view change delay and occurrence probability, consensus delay and throughput. The base station-enabled wireless PBFT network can achieve her consensus success probability, higher scalability, less power consumption, less communication complexity, and lower consensus delay than the wireless PBFT network using the IEEE 802.11 broadcast scheme. A special case with f deterministic Byzantine nodes and the optimal network configuration for achieving target consensus success probability are also presented to guide constructing a wireless PBFT network.

Chapter 5 delves into a more practical scenario where the wireless network is prone to crashes and malicious attacks. To cope with that, a hybrid PBFT network is investigated. The hybrid PBFT network consists of a private and a public cloud, where the nodes in the private cloud are prone only to crashes, while nodes in the public cloud are prone to both crashes and malicious attacks. The numerical results demonstrate that the hybrid PBFT network can achieve good security. If the private cloud is secure and immune to crashes, the security can be further enhanced.

The research findings have significant implications for the design and deployment of blockchain-enabled wireless networks:

- **Scalability Solutions:** The proposed base station-enabled PBFT frame-

work provides a scalable solution for deploying blockchain in wireless networks, particularly for IoT and smart city applications requiring large-scale participation.

- **Security Enhancements:** Hybrid PBFT networks offer a practical means of mitigating security risks in decentralized environments. This is particularly relevant for critical applications, such as healthcare and autonomous vehicles, where data integrity and fault tolerance are paramount.
- **Optimization Frameworks:** The analytical models and optimal configuration strategies presented can guide network operators in designing wireless blockchain systems that maximize performance while minimizing resource consumption.

The research also offers several broader insights for the integration of blockchain technology with wireless networks:

Consensus Mechanisms for Resource-Constrained Networks: After receiving a request from the client, the primary node broadcasts a *pre-prepare* message to all backup nodes.

- PBFT's voting-based approach, while less resource-intensive than proof-based mechanisms, still requires careful optimization to function effectively in wireless environments.
- The success of the proposed solutions highlights the need to adapt consensus algorithms to the unique constraints of wireless networks, such as limited bandwidth and higher failure probabilities.

Balancing Decentralization and Efficiency: The trade-off between decentralization and efficiency remains a critical challenge. The hybrid approach demonstrates that combining decentralized and centralized elements can strike a practical balance.

Interdisciplinary Collaboration: Effective deployment of wireless blockchain networks requires interdisciplinary collaboration, integrating insights from cryptography, communication theory, and distributed systems.

6.1 Future Works

This thesis explores the feasibility of deploying the PBFT consensus mechanism in the wireless network and provides practical guidance with different network

parameters. However, blockchain is a fast-developing technology with many aspects to be explored. With this regard, this thesis also discusses the possible research directions of blockchain for better adaption and deployment to the wireless network, which are listed as follows

- *Smart Contracts:* Smart contracts [133] are the basis of the blockchain, and they enable the automation of blockchain and reduce the reliability of the intermediate's fraud losses. Smart contracts research can be divided into two classes: development and evaluation [89]. Development refers to the smart contracts platform where the smart contracts are developed. Evaluation refers to performance and plausibility analysis. It can protect the blockchain from potential malfunctions or malicious attacks, increase the security level, and reduce loss. The advancement of smart contracts can improve blockchain's reliability and stability, but it still stays at a rudimentary stage, waiting for more exploration [134].

- *Wireless Network Construction:* More participants in the blockchain means a higher security level, more popularity, and more attractiveness, which can attract more users to join in and form a virtuous circle. The most influential factor will be the quality of the wireless network. A broader coverage brings more potential participants, and lower latency prevents the consensus process's failure and increases efficiency [11]. For example, in the PoW, successful mining needs to be broadcast as fast as possible to notify other miners to work on the next block; otherwise, double-spending or forking may happen.

- *Exploring Other Consensus Mechanisms:* Even though there are many existing consensus mechanisms [135], it seems that no single one can adapt to the wireless network and solve the problems solely. For example, PoW and PoS transaction rates may be the bottleneck, and PBFT is constrained by its scalability. A new consensus mechanism specifically designed for the wireless network is needed, or a controlling scheme that can flexibly switch the consensus mechanism according to the current network environment. The consensus success probability, throughput, latency, communication complexity and network traffic utilisation can be universal metrics for the performance evaluation.

- *The Trend to Decentralization:* The current centralised network structure has achieved unprecedented success, and its development is forecasted to continue in the coming years. This trend will impede the full

deployment of blockchain on the wireless network. Starting up the trend to decentralization will benefit the future deployment of blockchain on wireless networks [136].

- *Prevention and Recovery Mechanism:* Different blockchains have different weaknesses or are vulnerable to a variety of attacks. For example, in PBFT, when a primary fails, a new one will be selected to keep the system running according to the view change rule. This rule provides liveness to PBFT. Similar prevention or recovery mechanisms should be investigated to enhance the robustness and security of blockchain [137, 138].

- *Privacy preservation:* Even though blockchain technology can provide immutability and transparency to the data, privacy leakage is a rising concern because any blockchain participant can access the data stored in the blockchain. Cryptography, such as zero-knowledge proof, is a promising technique for coping with this problem [139, 140].

- *Scalability enhancement:* Scalability affects the deployment of the blockchain, especially when an extensive amount of users participate. Various efforts can be made to mitigate the scalability issue, such as sharding [141, 142], side chain [143] and off-chain [144, 145] techniques, and new chain structure like DAG [146].

- *Mobility:* In the IoT network, many devices can be mobile [147], such as wearable devices on people, intelligent vehicles, and drones. Most of the research focuses on the static situation. The generalisation of such research will be improved if the mobility issue is considered.

Bibliography

[1] IBM Institute for Business Value, "Device democracy: Saving the future of the internet of things," https://www.ibm.com/services/us/gbs/thoughtleadership/internetofthings/, 2015, [Online; accessed 10-December-2020].

[2] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6g wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 957–975, 2020.

[3] C. Yang, D. Puthal, S. P. Mohanty, and E. Kougianos, "Big-sensing-data curation for the cloud is coming: A promise of scalable cloud-data-center mitigation for next-generation iot and wireless sensor networks," *IEEE Consumer Electronics Magazine*, vol. 6, no. 4, pp. 48–56, 2017.

[4] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, "Distributed resource allocation and computation offloading in fog and cloud networks with non-orthogonal multiple access," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12 137–12 151, 2018.

[5] S. Joshi, A. A. Pise, M. Shrivastava, C. Revathy, H. Kumar, O. Alsetoohy, and R. Akwafo, "Adoption of blockchain technology for privacy and security in the context of industry 4.0," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 4079781, 2022.

[6] S. Kim, R. Shrestha, S. Kim, and R. Shrestha, "Security and privacy in intelligent autonomous vehicles," *Automotive Cyber Security: Introduction, Challenges, and Standardization*, pp. 35–66, 2020.

[7] B. Martínez-Pérez, I. De La Torre-Díez, and M. López-Coronado, "Privacy and security in mobile health apps: a review and recommendations," *Journal of medical systems*, vol. 39, pp. 1–8, 2015.

[8] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical internet of things: a review," *Security and Communication Networks*, vol. 2018, no. 1, p. 5978636, 2018.

[9] D. Gavidia and M. van Steen, "A probabilistic replication and storage scheme for large wireless networks of small devices," in *2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*. IEEE, 2008, pp. 469–476.

[10] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6g: Challenges, opportunities and research directions," *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1–5, 2020.

[11] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain-enabled wireless communications: a new paradigm towards 6g," *National science review*, vol. 8, no. 9, p. nwab069, 2021.

[12] Y. Wu, X. Gao, S. Zhou, W. Yang, Y. Polyanskiy, and G. Caire, "Massive access for future wireless communication systems," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 148–156, 2020.

[13] S. K. Das, V. Maheswari, and A. Sharma, "Wireless networks: Applications, challenges, and security issues," *Architectural Wireless Networks Solutions and Security Issues*, pp. 1–10, 2021.

[14] R. Nazir, A. A. Laghari, K. Kumar, S. David, and M. Ali, "Survey on wireless network security," *Archives of Computational Methods in Engineering*, pp. 1–20, 2021.

[15] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5g and beyond networks: A state of the art survey," *Journal of Network and Computer Applications*, vol. 166, p. 102693, 2020.

[16] S. Kharche and P. Dere, "Interoperability issues and challenges in 6g networks." *J. Mobile Multimedia*, vol. 18, no. 5, pp. 1445–1470, 2022.

[17] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[18] ——, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[19] M. Onik, M. Miraz, and C.-S. Kim, "A recruitment and human resource management technique using blockchain technology for industry 4.0," in *Smart Cities Symposium 2018*. Institution of Engineering and Technology, 2018.

[20] X. Wang, L. Feng, H. Zhang, C. Lyu, L. Wang, and Y. You, "Human resource information management model based on blockchain technology," in *2017 IEEE symposium on service-oriented system engineering (SOSE)*. IEEE, 2017.

[21] T. Hu, B. Xin, X. Liu, T. Chen, K. Ding, and X. Zhang, "Tracking the insider attacker: A blockchain traceability system for insider threats," *Sensors*, vol. 20, no. 18, p. 5297, sep 2020.

[22] O. B. Mora, R. Rivera, V. M. Larios, J. R. Beltrán-Ramírez, R. Maciel, and A. Ochoa, "A use case in cybersecurity based in blockchain to deal with the security and privacy of citizens and smart cities cyberinfrastructures," in *2018 IEEE International Smart Cities Conference (ISC2)*. IEEE, 2018, pp. 1–4.

[23] F. S. Ali, M. Aloqaily, O. Alfandi, and O. Ozkasap, "Cyberphysical blockchain-enabled peer-to-peer energy trading," *Computer*, vol. 53, no. 9, pp. 56–65, sep 2020.

[24] M. Baza, M. Nabil, M. Ismail, M. Mahmoud, E. Serpedin, and M. A. Rahman, "Blockchain-based charging coordination mechanism for smart grid energy storage units," in *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 504–509.

[25] Y. Liu, Z. Ai, S. Sun, S. Zhang, Z. Liu, and H. Yu, *FedCoin: A Peer-to-Peer Payment System for Federated Learning*. Cham: Springer International Publishing, 2020, pp. 125–138.

[26] L. Zhong, Q. Wu, J. Xie, J. Li, and B. Qin, "A secure versatile light payment system based on blockchain," *Future Generation Computer Systems*, vol. 93, pp. 327–337, 2019.

[27] L.-A. Hîrţan, C. Dobre, and H. González-Vélez, "Blockchain-based reputation for intelligent transportation systems," *Sensors*, vol. 20, no. 3, p. 791, 2020.

[28] R. Casado-Vara, P. Chamoso, F. De la Prieta, J. Prieto, and J. M. Corchado, "Non-linear adaptive closed-loop control system for improved efficiency in iot-blockchain management," *Information Fusion*, vol. 49, pp. 227–239, 2019.

[29] M. Poongodi, A. Sharma, V. Vijayakumar, V. Bhardwaj, A. P. Sharma, R. Iqbal, and R. Kumar, "Prediction of the price of ethereum blockchain

cryptocurrency in an industrial finance system," *Computers & Electrical Engineering*, vol. 81, p. 106527, 2020.

[30] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable multi-layer pbft consensus for blockchain," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 5, pp. 1146–1160, 2020.

[31] A. Rosic, "What is blockchain technology? a step-by-step guide for beginners," https://blockgeeks.com/guides/what-is-blockchain-technology/, [Online; accessed 14-December-2020].

[32] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *ieee vehicular technology magazine*, vol. 13, no. 1, pp. 32–39, 2018.

[33] J. Zarrin, H. Wen Phang, L. Babu Saheer, and B. Zarrin, "Blockchain for decentralization of internet: prospects, trends, and challenges," *Cluster Computing*, vol. 24, no. 4, pp. 2841–2866, 2021.

[34] S. Kekki, W. Featherstone, Y. Fang, P. Kuure, A. Li, A. Ranjan, D. Purkayastha, F. Jiangping, D. Frydman, G. Verin *et al.*, "Mec in 5g networks," *ETSI white paper*, vol. 28, no. 2018, pp. 1–28, 2018.

[35] D. D. Shin, "Blockchain: The emerging technology of digital trust," *Telematics and informatics*, vol. 45, p. 101278, 2019.

[36] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," *Journal of network and computer applications*, vol. 166, p. 102731, 2020.

[37] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.

[38] B. Cao, L. Zhang, M. Peng, and M. A. Imran, *Wireless blockchain: Principles, technologies and applications*. John Wiley & Sons, 2021.

[39] H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, "Blockchain-enabled resource management and sharing for 6g communications," *Digital Communications and Networks*, vol. 6, no. 3, pp. 261–269, 2020.

[40] H. T. Vo, A. Kundu, and M. K. Mohania, "Research directions in blockchain data management and analytics." in *EDBT*, 2018, pp. 445–448.

[41] J. Wan, J. Li, M. Imran, D. Li *et al.*, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3652–3660, 2019.

[42] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, and M. Pustišek, "Towards decentralized iot security enhancement: A blockchain approach," *Computers & Electrical Engineering*, vol. 72, pp. 266–273, 2018.

[43] T. Maksymyuk, J. Gazda, M. Volosin, G. Bugar, D. Horvath, M. Klymash, and M. Dohler, "Blockchain-empowered framework for decentralized network management in 6g," *IEEE Communications Magazine*, vol. 58, no. 9, pp. 86–92, 2020.

[44] A. Zwitter and J. Hazenberg, "Decentralized network governance: blockchain technology and the future of regulation," *Frontiers in Blockchain*, vol. 3, p. 12, 2020.

[45] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *Acm Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–41, 2021.

[46] P. Lafourcade and M. Lombard-Platet, "About blockchain interoperability," *Information Processing Letters*, vol. 161, p. 105976, 2020.

[47] H.-Y. Paik, X. Xu, H. D. Bandara, S. U. Lee, and S. K. Lo, "Analysis of data management in blockchain-based systems: From architecture to governance," *Ieee Access*, vol. 7, pp. 186 091–186 107, 2019.

[48] Q. Wei, B. Li, W. Chang, Z. Jia, Z. Shen, and Z. Shao, "A survey of blockchain data management systems," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 21, no. 3, pp. 1–28, 2022.

[49] K. Werbach, *The blockchain and the new architecture of trust*. Mit Press, 2018.

[50] O. Onireti, L. Zhang, and M. A. Imran, "On the viable area of wireless practical byzantine fault tolerance (pbft) blockchain networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[51] H. Luo, X. Yang, H. Yu, G. Sun, B. Lei, and M. Guizani, "Performance analysis and comparison of non-ideal wireless pbft and raft consensus networks in 6g communications," *IEEE Internet of Things Journal*, 2023.

[52] H. Luo, X. Yang, H. Yu, G. Sun, S. Xu, and L. Luo, "Performance analysis of non-ideal wireless pbft networks with mmwave and terahertz signals," in *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*. IEEE, 2023.

[53] H. Luo, G. Sun, H. Yu, B. Lei, and M. Guizani, "An energy-efficient wireless blockchain sharding scheme for pbft consensus," *IEEE Transactions on Network Science and Engineering*, 2024.

[54] Y. Sun, L. Zhang, P. Klaine, B. Cao, and M. Ali Imran, "Performance analysis on wireless blockchain iot system," *Wireless Blockchain: Principles, Technologies and Applications*, pp. 179–199, 2021.

[55] H. Xu, Y. Fan, W. Li, and L. Zhang, "Wireless distributed consensus for connected autonomous systems," *IEEE Internet of Things Journal*, 2022.

[56] C. Feng, Z. Xu, X. Zhu, P. V. Klaine, and L. Zhang, "Wireless distributed consensus in vehicle to vehicle networks for autonomous driving," *IEEE Transactions on Vehicular Technology*, 2023.

[57] S. Gao, T. Yu, J. Zhu, and W. Cai, "T-pbft: An eigentrust-based practical byzantine fault tolerance consensus algorithm," *China Communications*, vol. 16, no. 12, pp. 111–123, 2019.

[58] Y. Li, Y. Fan, L. Zhang, and J. Crowcroft, "Raft consensus reliability in wireless networks: Probabilistic analysis," *IEEE Internet of Things Journal*, 2023.

[59] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Network*, vol. 32, no. 3, pp. 78–83, 2018.

[60] S. Underwood, "Blockchain beyond bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[61] P. Bhattacharya, S. Tanwar, R. Shah, and A. Ladha, "Mobile edge computing-enabled blockchain framework—a survey," in *Proceedings of ICRIC 2019*. Springer, 2020, pp. 797–809.

[62] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[63] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner, "Ripple: Overview and outlook," in *International Conference on Trust and Trustworthy Computing*. Springer, 2015, pp. 163–180.

[64] A. Baliga, I. Subhod, P. Kamat, and S. Chatterjee, "Performance evaluation of the quorum blockchain platform," *arXiv preprint arXiv:1809.03421*, 2018.

[65] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn, "Corda: an introduction," *R3 CEV, August*, vol. 1, no. 15, p. 14, 2016.

[66] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, vol. 154, p. 113385, 2020.

[67] J. Xu, C. Wang, and X. Jia, "A survey of blockchain consensus protocols," *ACM Computing Surveys*, vol. 55, no. 13s, pp. 1–35, 2023.

[68] P. R. Nair and D. R. Dorai, "Evaluation of performance and security of proof of work and proof of stake using blockchain," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*. IEEE, 2021, pp. 279–283.

[69] R. Chen, I.-P. Tu, K.-E. Chuang, Q.-X. Lin, S.-W. Liao, and W. Liao, "Endex: Degree of mining power decentralization for proof-of-work based blockchain systems," *IEEE Network*, vol. 34, no. 6, pp. 266–271, 2020.

[70] J. Yun, Y. Goh, and J.-M. Chung, "Analysis of mining performance based on mathmatical approach of pow," in *2019 International Conference on Electronics, Information, and Communication (ICEIC)*. IEEE, 2019, pp. 1–2.

[71] J. Debus, "Consensus methods in blockchain systems," *Frankfurt School of Finance & Management, Blockchain Center, Tech. Rep*, 2017.

[72] M. Salimitari and M. Chatterjee, "A survey on consensus protocols in blockchain for iot networks," *arXiv preprint arXiv:1809.05613*, 2018.

[73] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance."

[74] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems (TOCS)*, vol. 20, no. 4, pp. 398–461, 2002.

[75] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric)," in *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*. IEEE, 2017, pp. 253–255.

[76] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14)*, 2014, pp. 305–319.

[77] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE international conference on systems, man, and cybernetics (SMC)*. IEEE, 2017, pp. 2567–2572.

[78] D. Huang, X. Ma, and S. Zhang, "Performance analysis of the raft consensus algorithm for private blockchains," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 172–181, 2019.

[79] S. Popov, "The tangle," *cit. on*, vol. 131, 2016.

[80] K. Sharma and D. Jain, "Consensus algorithms in blockchain technology: a survey," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2019, pp. 1–7.

[81] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *Ieee Access*, vol. 7, pp. 22 328–22 370, 2019.

[82] B. CURRAN, "What is the tangle? complete guide to iota's directed acyclic graph (dag)," https://blockonomi.com/iota-tangle/, 2018, [Online; accessed 25-January-2020].

[83] 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*, vol. 6, no. 3, pp. 5791–5802, 2019.

[84] H. Xu, L. Zhang, Y. Liu, and B. Cao, "RAFT Based Wireless Blockchain Networks in the Presence of Malicious Jamming," *IEEE Wireless Communications Letters*, vol. 9, no. 6, pp. 817–821, jun 2020.

[85] D. Yu, W. Li, H. Xu, and L. Zhang, "Low Reliable and Low Latency Communications for Mission Critical Distributed Industrial Internet of Things," *IEEE Communications Letters*, vol. 25, no. 1, pp. 313–317, jan 2021.

[86] D. Yang, C. Long, H. Xu, and S. Peng, "A review on scalability of blockchain," in *Proceedings of the 2020 2nd International Conference on Blockchain Technology*, 2020, pp. 1–6.

[87] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *Ieee Access*, vol. 8, pp. 16 440–16 455, 2020.

[88] S. K. Singh, S. Rathore, and J. H. Park, "Blockiotintelligence: A blockchain-enabled intelligent iot architecture with artificial intelligence," *Future Generation Computer Systems*, vol. 110, pp. 721–743, 2020.

[89] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, "Convergence of blockchain and artificial intelligence in iot network for the sustainable smart city," *Sustainable Cities and Society*, vol. 63, p. 102364, 2020.

[90] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The energy consumption of blockchain technology: Beyond myth," *Business & Information Systems Engineering*, vol. 62, no. 6, pp. 599–608, 2020.

[91] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 3–16.

[92] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Network*, vol. 33, no. 5, pp. 166–173, 2019.

[93] C. Huang, Z. Wang, H. Chen, Q. Hu, Q. Zhang, W. Wang, and X. Guan, "Repchain: A reputation-based secure, fast, and high incentive blockchain system via sharding," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4291–4304, 2020.

[94] J. Moubarak, E. Filiol, and M. Chamoun, "On blockchain security and relevant attacks," in *2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)*. IEEE, 2018, pp. 1–6.

[95] S. Alqahtani and M. Demirbas, "Bottlenecks in blockchain consensus protocols," in *2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS)*. IEEE, 2021, pp. 1–8.

[96] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5g-enabled iot for industrial automation: A systematic review, solutions, and challenges," *Mechanical systems and signal processing*, vol. 135, p. 106382, 2020.

[97] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6g wireless networks: Vision, requirements, architecture, and key technologies," *IEEE vehicular technology magazine*, vol. 14, no. 3, pp. 28–41, 2019.

[98] F. Salahdine, T. Han, and N. Zhang, "5g, 6g, and beyond: Recent advances and future challenges," *Annals of Telecommunications*, vol. 78, no. 9, pp. 525–549, 2023.

[99] A. Gohar and G. Nencioni, "The role of 5g technologies in a smart city: The case for intelligent transportation system," *Sustainability*, vol. 13, no. 9, p. 5188, 2021.

[100] T. Rathod, N. K. Jadav, M. D. Alshehri, S. Tanwar, R. Sharma, R.-A. Felseghi, and M. S. Raboaca, "Blockchain for future wireless networks: A decade survey," *Sensors*, vol. 22, no. 11, p. 4182, 2022.

[101] C. Bendiksen, S. Gibbons, and E. Lim, "The bitcoin mining network-trends, marginal creation cost, electricity consumption & sources," *CoinShares Research*, vol. 21, pp. 3–19, 2018.

[102] J. C.-P. Wang, M. Abolhasan, D. R. Franklin, and F. Safaei, "Characterising the behaviour of ieee 802.11 broadcast transmissions in ad hoc wireless lans," in *2009 IEEE International Conference on Communications*, 2009, pp. 1–5.

[103] F. Daneshgaran, M. Laddomada, F. Mesiti, and M. Mondin, "Unsaturated throughput analysis of ieee 802.11 in presence of non ideal transmission channel and capture effects," *IEEE transactions on Wireless Communications*, vol. 7, no. 4, pp. 1276–1286, 2008.

[104] X. Ma and X. Chen, "Performance analysis of ieee 802.11 broadcast scheme in ad hoc wireless lans," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3757–3768, 2008.

[105] G. Wang, Y. Shu, L. Zhang, and O. W. Yang, "Delay analysis of the ieee 802.11 dcf," in *14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003.*, vol. 2. IEEE, 2003, pp. 1737–1741.

[106] sawtooth, "Pbft architecture — sawtooth pbft 0.1 documentation," https://sawtooth.hyperledger.org/docs/1.2/pbft/architecture.html.

[107] Z. Zhou, O. Onireti, L. Zhang, and M. A. Imran, "Performance analysis of wireless practical byzantine fault tolerance networks using ieee 802.11," in *2021 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2021, pp. 1–6.

[108] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535–547, Mar. 2000.

[109] M. Nischwitz, M. Esche, and F. Tschorsch, "Bernoulli meets pbft: Modeling bft protocols in the presence of dynamic failures," in *2021 16th Conference on Computer Science and Intelligence Systems (FedCSIS)*. IEEE, 2021, pp. 291–300.

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

[111] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," in *Concurrency: the works of leslie lamport*, 2019, pp. 203–226.

[112] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375, 2018.

[113] Y. Lai, L. Tong, J. Liu, Y. Wang, T. Tang, Z. Zhao, and H. Qin, "Identifying malicious nodes in wireless sensor networks based on correlation detection," *Computers & Security*, vol. 113, p. 102540, 2022.

[114] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Transactions on communications*, vol. 59, no. 11, pp. 3122–3134, 2011.

[115] T. D. Novlan, H. S. Dhillon, and J. G. Andrews, "Analytical modeling of uplink cellular networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2669–2679, 2013.

[116] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic geometry and its applications*. John Wiley & Sons, 2013.

[117] K. James F, R. Keith W *et al.*, *Computer Networking: A Top-Down Approach.-6th*. Addison-Wesley, 2013.

[118] A. Roy, J. L. Pachuau, and A. K. Saha, "An overview of queuing delay and various delay based algorithms in networks," *Computing*, vol. 103, no. 10, pp. 2361–2399, 2021.

[119] D. Bertsekas and R. Gallager, *Data networks*. Athena Scientific, 2021.

[120] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[121] W. Feller, *An introduction to probability theory and its applications, Volume 2*. John Wiley & Sons, 1991, vol. 81.

[122] D. Bertsekas and J. N. Tsitsiklis, *Introduction to probability*. Athena Scientific, 2008, vol. 1.

[123] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 121–130.

[124] E. Zeljković, N. Slamnik-Kriještorac, S. Latré, and J. M. Marquez-Barja, "Abraham: machine learning backed proactive handover algorithm using sdn," *IEEE Transactions on Network and Service Management*, vol. 16, no. 4, pp. 1522–1536, 2019.

[125] H. Luo, X. Yang, H. Yu, G. Sun, B. Lei, and M. Guizani, "Performance analysis and comparison of non-ideal wireless pbft and raft consensus networks in 6g communications," *IEEE Internet of Things Journal*, 2023.

[126] M. J. Amiri, S. Maiyya, D. Agrawal, and A. El Abbadi, "Seemore: A fault-tolerant protocol for hybrid cloud environments," in *2020 IEEE 36th International Conference on Data Engineering (ICDE)*. IEEE, 2020, pp. 1345–1356.

[127] T. Mitani and A. Otsuka, "Traceability in permissioned blockchain," *IEEE Access*, vol. 8, pp. 21 573–21 588, 2020.

[128] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: A comparison," *Ict Express*, vol. 7, no. 2, pp. 229–233, 2021.

[129] M. U. Hassan, M. H. Rehmani, and J. Chen, "Anomaly detection in blockchain networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 289–318, 2022.

[130] N. R. Pradhan and A. P. Singh, "Smart contracts for automated control system in blockchain based smart cities," *Journal of Ambient Intelligence and Smart Environments*, vol. 13, no. 3, pp. 253–267, 2021.

[131] R. Han, Z. Yan, X. Liang, and L. T. Yang, "How can incentive mechanisms and blockchain benefit with each other? a survey," *ACM Computing Surveys*, vol. 55, no. 7, pp. 1–38, 2022.

[132] Z. Zhou, X. Chen, Y. Zhang, and S. Mumtaz, "Blockchain-empowered secure spectrum sharing for 5g heterogeneous networks," *IEEE Network*, vol. 34, no. 1, pp. 24–31, 2020.

[133] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-peer Networking and Applications*, vol. 14, pp. 2901–2925, 2021.

[134] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *2018 9th international conference on computing, communication and networking technologies (ICCCNT)*. IEEE, 2018, pp. 1–4.

[135] S. Zhou, K. Li, L. Xiao, J. Cai, W. Liang, and A. Castiglione, "A systematic review of consensus mechanisms in blockchain," *Mathematics*, vol. 11, no. 10, p. 2248, 2023.

[136] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*. Ieee, 2017, pp. 557–564.

[137] H. Zhao, Y. Zhang, Y. Peng, and R. Xu, "Lightweight backup and efficient recovery scheme for health blockchain keys," in *2017 IEEE 13th international symposium on autonomous decentralized system (ISADS)*. IEEE, 2017, pp. 229–234.

[138] W. Liang, Y. Fan, K.-C. Li, D. Zhang, and J.-L. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6543–6552, 2020.

[139] X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie, and X. Peng, "A survey on zero-knowledge proof in blockchain," *IEEE network*, vol. 35, no. 4, pp. 198–205, 2021.

[140] D. Čapko, S. Vukmirović, and N. Nedić, "State of the art of zero-knowledge proofs in blockchain," in *2022 30th Telecommunications Forum (TELFOR)*. IEEE, 2022, pp. 1–4.

[141] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in *2018 IEEE symposium on security and privacy (SP)*. IEEE, 2018, pp. 583–598.

[142] J. Wang and H. Wang, "Monoxide: Scale out blockchains with asynchronous consensus zones," in *16th USENIX symposium on networked systems design and implementation (NSDI 19)*, 2019, pp. 95–112.

[143] J. Poon and V. Buterin, "Plasma: Scalable autonomous smart contracts," *White paper*, pp. 1–47, 2017.

[144] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten, "Arbitrum: Scalable, private smart contracts," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 1353–1370.

[145] J. Teutsch and C. Reitwießner, "A scalable verification solution for blockchains," in *Aspects of Computation and Automata Theory with Applications*. World Scientific, 2024, pp. 377–424.

[146] Y. Sompolinsky and A. Zohar, "Phantom," *IACR Cryptology ePrint Archive, Report 2018/104*, 2018.

[147] S. M. Ghaleb, S. Subramaniam, Z. A. Zukarnain, and A. Muhammed, "Mobility management for iot: a survey," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, pp. 1–25, 2016.